

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

[19]中华人民共和国国家知识产权局

[51]Int. Cl⁶

H04N 5/913

G11B 20/10 H04N 7/50

[12] 发明专利申请公开说明书

[21] 申请号 99103282.9

[43]公开日 1999年12月22日

[11]公开号 CN 1239378A

[22]申请日 99.1.27 [21]申请号 99103282.9

[30]优先权

[32]98.1.27 [33]JP [31]013935/98

[32]98.1.27 [33]JP [31]013954/98

[32]98.1.27 [33]JP [31]013955/98

[71]申请人 佳能株式会社

地址 日本东京

[72]发明人 岩村惠市

[74]专利代理机构 中国国际贸易促进委员会专利商标事
务所

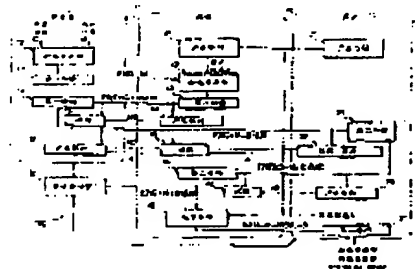
代理人 马 浩

权利要求书 10 页 说明书 63 页 附图页数 24 页

[54]发明名称 电子水印方法、信息分发系统、图象编档装
置和存储介质

[57]摘要

一种用于在一个网络上交换数据的电子信息分发系统,该系统至少包括:包括第一加密装置的第一实体,用于对原始数据执行第一加密处理;包括管理分发装置的第二实体,用于至少是管理或分发通过所述第一加密处理提供的的数据,还包括一个电子水印嵌入装置,用于在所述数据中嵌入一个电子水印;第三实体,包括用于对其中已经嵌入一个电子水印的数据执行第二加密的第二加密装置。



ISSN 1008-4274

权 利 要 求 书

1. 一种电子水印方法, 包括:

第一步骤, 在该步骤处, 第一实体执行对原始数据的第一加密处理;

第二步骤, 在该步骤处, 第二实体至少是管理或分发通过所述第一加密提供的所述数据并将一个电子水印嵌入到所述数据中; 和

第三步骤, 在该步骤处, 第三实体对已经被嵌入所述电子水印的所述数据执行第二加密处理。

2. 根据权利要求1所述的电子水印方法, 其特征是所述第一步骤至少包括在对所述原始数据执行所述第一加密之前或之后嵌入一个电子水印的步骤。

3. 根据权利要求1所述的电子水印方法, 其特征是所述第二步骤至少包括在嵌入所述电子水印之前或之后执行第三加密处理的步骤。

4. 根据权利要求1所述的电子水印方法, 其特征是还包括如下步骤: 分发至少受所述第一加密处理或第二加密处理影响的, 和所述电子水印被嵌入在其中的数据。

5. 根据权利要求1所述的电子水印方法, 其特征是还包括如下步骤: 证书办公室使用伴有一个证书的匿名公共密钥检查用于所述第三实体的签名。

6. 根据权利要求1所述的电子水印方法, 其特征是所述第二实体包括多个实体。

7. 根据权利要求1所述的电子水印方法, 其特征是被所述第二实体嵌入的信息是涉及所述第三实体的信息或是涉及将被传送数据的信息。

8. 根据权利要求1所述的电子水印方法, 其特征是所述第一步骤包括至少是在对所述原始数据执行所述第一加密处理之前或之后将一个电子水印嵌入到图象数据中的步骤, 和其中, 将由第 n ($n \geq 1$) 实体嵌入的信息是涉及第 $(n+1)$ 实体的信息或涉及将被传送的数据的信息。

9. 根据权利要求1或2所述的电子水印方法, 其特征是所述用于嵌入所述电子水印的处理是不用于嵌入涉及所述第二实体的信息的处理。

10. 根据权利要求1或2所述的电子水印方法, 其特征是所述原始数据是图象数据。

11. 一种在网络上交换数据的电子信息分发系统, 至少包括:

第一实体, 包括第一加密装置, 用于执行对所述原始数据的第一加密处

理;

第二实体, 包括一个用于至少管理或分发由所述第一加密处理提供的所述数据的管理分发装置, 和一个用于在所述数据中嵌入所述电子水印的电子水印嵌入装置; 和

第三实体, 包括用于对已经被嵌入一个电子水印的数据进行第二加密处理的第二加密装置。

12. 根据权利要求 11 所述的电子信息分发系统, 其特征是所述第一实体包括至少一个电子水印嵌入装置, 用于在执行对所述原始数据的所述第一加密处理之前或之后嵌入一个电子水印。

13. 根据权利要求 11 所述的电子信息分发系统, 其特征是所述第二实体包括至少第三加密装置, 用于在嵌入所述电子水印之前或之后执行第三加密处理。

14. 根据权利要求 11 所述的电子信息分发系统, 其特征是还包括:

分发装置, 用于分发至少受到所述第一加密处理或第二加密处理影响的, 所述电子水印被嵌入其中的数据。

15. 根据权利要求 11 所述的电子信息分发系统, 其特征是还包括:

验证装置, 用于使用带有由证书办公室颁发的证书的匿名公共密钥检查与所述第三实体相关的一个签名。

16. 根据权利要求 11 所述的电子信息分发系统, 其特征是所述第二实体包括多个实体。

17. 根据权利要求 11 所述的电子信息分发系统, 其特征是将被所述第二实体嵌入的信息是涉及所述第三实体的信息或涉及将被传送的数据的信息。

18. 根据权利要求 11 所述的电子信息分发系统, 其特征是所述第一实体包括一个电子水印嵌入装置, 用于在执行对所述原始数据的所述第一加密处理之前或之后在图象数据中嵌入一个电子水印; 和其中, 第 n ($n \geq 1$) 个实体的电子水印嵌入装置嵌入所述涉及第 $(n+1)$ 个实体的信息或涉及将被传送的数据的信息。

19. 根据权利要求 11 或 12 所述的电子信息分发系统, 其特征是所述电子水印嵌入装置不嵌入至少是涉及所述第二实体的信息。

20. 根据权利要求 11 所述的电子信息分发系统, 其特征是所述原始数据是图象数据。

21. 一种用于存储根据权利要求1到10之一的电子水印嵌入方法的步骤产生的数据的图彖编档装置。

22. 一种在其上存储了根据权利要求1到10之一的所述电子水印嵌入方法的步骤从而可由一个计算机读出的存储媒体。

23. 一种电子水印叠加方法, 包括如下步骤:

加密电子信息和交换所生成的电子信息;

在加密处理期间, 在所述电子水印中嵌入电子水印信息; 和

重复多次用于传送伴随有一个电子水印的所述电子信息的处理,

借此, 利用第一实体传送上面已经被叠加有所述电子水印信息的所述电子信息并经过第二实体传送给第三实体。

24. 根据权利要求23所述的电子水印叠加方法, 其特征是在所述的重复处理过程中, 在所述传送实体向所述接收实体传送所述电子信息之前, 所述传送实体在已经被所述接收实体加密的电子信息中嵌入一个电子水印。

25. 根据权利要求24所述的电子水印叠加方法, 其特征是在所述的重复处理过程中, 所述接收实体对已经由所述传送实体执行了不同于第二加密的第一加密的电子信息执行第二加密, 并且, 将所生成的信息返回给所述传送实体, 和其中, 所述传送实体解密所述电子信息的第一加密部分, 和嵌入所述电子水印信息。

26. 根据权利要求23所述的电子水印叠加方法, 其特征是在所述的重复处理过程中, 在所述传送实体向所述接收实体传送所述电子信息之前, 所述接收实体在已经被所述传送实体加密的电子信息中嵌入一个电子水印。

27. 根据权利要求26所述的电子水印叠加方法, 其特征是在所述重复处理过程中, 所述接收实体将一个电子水印信息加到已经由所述传送实体执行了第一加密的电子信息上, 并执行不同于所述第一加密的第二加密, 和将所生成的信息返回到所述传送实体, 其中, 所述传送实体解密其中已经被嵌入所述电子水印信息的所述电子信息的第一加密部分, 和将所生成的信息传送给所述接收实体。

28. 根据权利要求24到27中任何一个所述的电子水印叠加方法, 其特征是在加密所述电子信息之前, 所述传送实体在所述电子信息中嵌入一个不同的电子水印信息。

29. 根据权利要求28所述的电子水印叠加方法, 其特征是用于规定所述接

收实体的信息被作为所述电子水印信息嵌入。

30. 根据权利要求 24 到 29 中任何一个所述的电子水印叠加方法, 其特征是使用伴随有由所述证书办公室发出的证书的匿名公共密钥检查与所述接收实体相关的签名。

31. 根据权利要求 24 到 29 中任何一个所述的电子水印叠加方法, 其特征是当所述第三实体被用做一个接收实体时, 使用由所述证书办公室发出的匿名公共密钥检查与所述第三实体相关的签名, 和当所述第二实体被用做接收实体时, 使用由所述证书办公室发出的一个匿名公共密钥检查与所述第二实体相关的签名。

32. 一种电子信息分发系统, 包括:

其中保持原始电子信息的第一实体, 包括用于加密所述原始电子信息的加密装置和用于在由所述加密处理提供的电子信息中嵌入一个电子水印的嵌入装置;

第二实体, 包括用于管理和分发从所述第一实体接收的电子信息并用于加密所述电子信息的加密装置, 和包括用于在所述电子信息中嵌入电子水印信息的嵌入装置; 和

第三实体, 包括加密从所述第二实体接收的电子信息的加密装置, 用于使用所生成的电子信息。

33. 根据权利要求 32 所述的电子信息分发系统, 其特征是相同的处理至少被用做用于从所述第一实体向所述第二实体传送电子信息的第一过程的一部分或用于由所述第二实体向所述第三实体传送电子信息的第二过程的一部分。

34. 根据权利要求 33 所述的电子信息分发系统, 其特征是所述第一和第二实体、第二和第三实体加密所述电子信息并交换被加密的信息, 和在所述处理期间, 嵌入的电子水印信息。

35. 根据权利要求 33 或 34 所述的电子信息分发系统, 其特征是在所述相同的处理中, 在所述传送实体向所述接收实体传送所述电子信息之前, 所述传送实体在已经被所述接收实体加密的电子信息中嵌入一个电子水印。

36. 根据权利要求 35 所述的电子信息分发系统, 其特征是在所述相同处理中, 所述接收实体对已经由所述传送实体执行不同于第二加密的第一加密的电子信息执行第二加密, 并将所生成的信息返回到所述传送实体, 其中, 所述传

送实体解密所述电子信息的第一加密部分, 和嵌入所述电子水印信息。

37. 根据权利要求 33 或 34 所述的电子信息分发系统, 其特征是在所述相同的处理中, 在所述传送实体向所述接收实体传送所述电子信息之前, 所述接收实体在由所述传送实体加密的电子信息中嵌入一个电子水印。

38. 根据权利要求 37 所述的电子信息分发系统, 其特征是在所述相同的处理中, 所述接收实体将电子水印信息加到已经由所述传送实体执行了第一加密的电子信息上, 并执行不同于所述第一加密的第二加密, 和将所生成的信息返回到所述传送实体, 其中, 所述传送实体解密其中已经被嵌入所述电子水印信息的所述电子信息的第一加密部分, 和将所生成的信息传送给所述接收实体。

39. 根据权利要求 33 到 38 中任何一个所述的电子信息分发系统, 其特征是在所述相同的处理中, 在加密所述电子信息之前, 所述传送实体在所述电子信息中嵌入不同的电子水印信息。

40. 根据权利要求 33 到 39 中任何一个所述的电子信息分发系统, 其特征是使用具有由证书办公室颁发的证书的匿名公共密钥检查与所述接收实体相关的签名。

41. 根据权利要求 32 到 39 中任何一个所述的电子信息分发系统, 其特征是当所述第三实体被用做一个接收实体时, 使用由所述证书办公室颁发的匿名公共密钥检查与所述第三实体相关的签名, 和当所述第二实体被用做一个接收实体时, 使用由所述证书办公室颁发的匿名公共密钥检查与所述第二实体相关的签名。

42. 一种电子水印叠加方法, 用于由传送实体向接收实体传送电子信息, 所述传送实体重复对已经被所述接收实体加密的电子信息执行的电子水印处理, 从而由第一实体经过第二实体向第三实体至少传送上面已经被叠加有一个电子水印的电子信息。

43. 一种电子水印叠加方法, 包括如下步骤:

一个传送实体对电子信息执行第一加密处理;

一个接收实体对所生成的电子信息执行不同于所述第一加密的第二加密, 和将所获得的电子信息返回到所述传送实体; 和

所述传送实体解密已经被执行所述第一加密的所述电子信息, 和在已经被解密的所述电子信息中嵌入电子水印信息,

其中, 通过重复上述步骤, 上面已经被叠加有所述电子水印信息的电子信

息被至少从第一实体经过第二实体传送给第三实体。

44. 一种电子信息分发系统, 包括:

用于保持原始电子信息的第一实体;

第二实体, 用于管理和分发从所述第一实体接收的电子信息; 和

第三实体, 用于使用从所述第二实体接收的所述电子信息,

其中, 为了由传送实体向接收实体传送电子信息, 所述传送实体重复用于在电子信息中嵌入一个电子水印信息的处理, 从而由所述第一实体经过第二实体向第三实体至少传送其中已经被嵌入电子水印信息的电子信息。

45. 一种电子信息分发系统, 包括:

用于保持原始电子信息的第一实体;

第二实体, 用于管理和分发所述第一实体接收的电子信息; 和

第三实体, 用于使用从所述第二实体接收的所述电子信息,

其中, 接收实体对已经由所述传送实体执行了不同于第二加密处理的第一加密处理的电子信息执行第二加密处理, 并将所生成的电子信息返回到所述传送实体,

其中, 所述传送实体解密已经被执行了所述第一加密处理的电子信息, 并在所生成的电子信息中嵌入所述电子水印信息, 和

其中, 通过重复所述处理, 由所述第一实体经过第二实体向第三实体至少传送上面已经被叠加有电子水印信息的电子信息。

46. 一种电子水印方法, 包括如下步骤:

使用多个装置或实体执行用于加密和用于嵌入一个电子水印的分发式处理; 和

使用附加的装置或实体检查至少由所述多个装置或实体执行的所述加密处理或用于嵌入一个电子水印的处理的合法性。

47. 根据权利要求 46 所述的电子水印方法, 其特征是所述多个装置或实体是:

包括第一加密装置的第一实体;

包括电子水印嵌入装置的第二实体, 用于管理和分发从所述第一实体接收的数据; 和

包括第二加密装置的第三实体, 用于使用其中已经嵌入一个电子水印的数据。

48. 根据权利要求 46 所述的电子水印方法, 其特征是所述多个装置或实体是:

包括第一加密装置的第一实体;

包括电子水印嵌入装置的第二实体, 用于管理和分发从所述第一实体接收的数据; 和

包括电子水印嵌入装置和第二加密装置的第三实体, 用于使用其中已经嵌入一个电子水印的数据。

49. 根据权利要求 46 所述的电子水印方法, 其特征是所述多个装置或实体是:

包括第一电子水印装置和第一加密装置的第一实体;

包括电子水印嵌入装置的第二实体, 用于管理和分发从所述第一实体接收的数据; 和

包括第二加密装置的第三实体, 用于使用其中已经嵌入一个电子水印的数据。

50. 根据权利要求 46 所述的电子水印方法, 其特征是所述多个装置或实体是:

包括电子水印嵌入装置和第一加密装置的第一实体;

包括电子水印嵌入装置、第一加密装置和第二加密装置中至少一个的第二实体, 用于管理和分发从所述第一实体接收的数据; 和

包括电子水印嵌入装置和第二加密装置的第三实体, 用于使用其中已经嵌入一个电子水印的数据。

51. 根据权利要求 46 到 50 中任何一个所述的电子水印方法, 其特征是所述实体加密其中已经被嵌入一个电子水印的数据。

52. 根据权利要求 46 到 50 中任何一个所述的电子水印方法, 其特征是所述实体在已经加密的数据中嵌入一个电子水印。

53. 根据权利要求 46 到 50 中任何一个所述的电子水印方法, 其特征是所述第二实体在已经由所述第一实体执行了第一加密的数据中嵌入一个电子水印。

54. 根据权利要求 47 所述的电子水印方法, 其特征是所述第二实体在由所述第一实体执行了第一加密的数据中和在由所述第三实体执行了第二加密的数据中嵌入一个电子水印。

55. 根据权利要求 54 所述的电子水印方法, 其特征是所述第二实体输出通过使用单向函数变换所述第二加密数据获得的一个值。

56. 根据权利要求 55 所述的电子水印方法, 其特征是所述第二实体向所述第四实体传送通过使用所述单向函数进行变换所获得的一个值。

57. 根据权利要求 47 到 55 中任何一个所述的电子水印方法, 其特征是与所述第二加密数据一起, 所述第三实体输出使用所述单向函数对所述第二加密数据进行变换所获得的一个值。

58. 根据权利要求 57 所述的电子水印方法, 其特征是所述第三实体向所述第四实体传送使用所述单向函数进行变换所获得的一个值。

59. 根据权利要求 47 到 50 中任何一个所述的电子水印方法, 其特征是所述第三实体接收预先已经被执行第一加密的信息, 和执行所接收信息的第二加密。

60. 根据权利要求 47 到 50 中任何一个所述的电子水印方法, 其特征是所述第四实体能够执行与所述第二加密对应的解密。

61. 根据权利要求 47 到 50 中任何一个所述的电子水印方法, 其特征是所述第四实体包括一个用于管理一个加密密钥的装置。

62. 根据权利要求 61 所述的电子水印方法, 其特征是为了验证至少所述电子水印和所述加密处理的合法性, 所述第四实体解密在其中嵌入一个电子水印的同时被加密和由一个不同实体输出的数据。

63. 根据权利要求 61 或 62 所述的电子水印方法, 其特征是为了验证至少所述电子水印和所述加密处理的合法性, 所述第四实体将由所述不同实体输出的一个值与在其中嵌入一个水印的同时被加密和由该不同实体输出的所述数据进行比较。

64. 一种电子信息分发系统, 其特征是该系统用于在由多个实体构成的一个网络上交换数字数据, 所述系统包括:

包括第一数据加密装置的第一实体;

包括一个电子水印嵌入装置的第二实体, 用于管理和分发从所述第一实体接收的数据;

包括第二加密装置的第三实体, 用于使用其中已经被嵌入一个电子水印的数据; 和

第四实体, 用于检查至少由所述第一到第三实体执行的所述加密处理或电

子水印嵌入处理的合法性。

65. 一种电子信息分发系统，其特征是该系统用于在由多个实体构成的一个网络上交换数字数据，所述系统包括：

包括第一数据加密装置的第一实体；

包括电子水印嵌入装置的第二实体，用于管理和分发从所述第一实体接收的数据；

包括电子水印嵌入装置和第二加密装置的第三实体，用于使用其中已经被嵌入一个电子水印的数据；

第四实体，用于检查至少由所述加密处理或由所述第一到第三实体执行的所述电子水印嵌入处理的合法性。

66. 一种电子信息分发系统，其特征是该系统用于在由多个实体构成的一个网络上交换数字数据，所述系统包括：

包括电子水印嵌入装置和第一数据加密装置的第一实体；

包括电子水印嵌入装置的第二实体，用于管理和分发从所述第一实体接收的数据；

包括第二加密装置的第三实体，用于使用其中已经被嵌入一个电子水印的数据；和

第四实体，用于检查至少由所述第一到第三实体执行的所述加密处理或所述电子水印嵌入处理的合法性。

67. 一种电子信息分发系统，其特征是该系统用于在由多个实体构成的一个网络上交换数字数据，所述系统包括：

包括电子水印嵌入装置和第一数据加密装置的第一实体；

包括所述电子水印嵌入装置、第一加密装置和第二加密装置中至少一个的第二实体，用于管理和分发从所述第一实体接收的数据；

包括电子水印嵌入装置和第二加密装置的第三实体，用于使用其中已经嵌入一个电子水印的数据；

第四实体，用于检查至少由所述第一到第三实体执行的所述加密处理或所述电子水印嵌入处理的合法性。

68. 根据权利要求 64 到 67 中任何一个所述的电子信息分发系统，其特征是用于执行验证的所述第四实体能够执行与所述第二加密对应的解密。

69. 根据权利要求 66 或 67 所述的电子信息分发系统，其特征是将被所述

第一实体嵌入的所述电子水印信息包括涉及所述第三实体的信息。

70. 根据权利要求 66 或 67 所述的电子信息分发系统，其特征是将被所述第一实体嵌入的所述电子水印信息包括涉及将被传送的数字数据的信息。

71. 根据权利要求 64 到 67 中任何一个所述的电子信息分发系统，其特征是将被所述第一实体嵌入的所述电子水印信息包括涉及所述第三实体的信息。

72. 根据权利要求 65 或 67 所述的电子信息分发系统，其特征是将被所述第三实体嵌入的所述电子水印信息包括只能由所述第三实体准备的信息。

73. 根据权利要求 65 或 67 所述的电子信息分发系统，其特征是在使用伴有由所述证书办公室颁发的证书的匿名公共密钥验证与所述第三实体相关的签名之后，所述第一实体嵌入所述电子水印。

74. 根据权利要求 64 到 67 中任何一个所述的电子信息分发系统，其特征是在使用伴有由所述证书办公室颁发的证书的匿名公共密钥验证与所述第三实体相关的签名之后，所述第二实体嵌入所述电子水印。

说明书

电子水印方法、信息分发系统、 图象编档装置和存储介质

本发明涉及一种电子水印方法、电子信息分发系统、图象编档装置和上面存储有用于执行电子水印方法的步骤并可以被计算机读出的存储介质。特别是，本发明涉及一种用于保护诸如运动图象数据、静态图象数据、音频数据、计算机数据和计算机程序的数字信息的版权的电子水印方法、用于使用所述电子水印方法分发数字信息的诸如多媒体网络系统的电子信息分发系统、使用所述电子水印方法的图象编档系统和上面存储有用于执行所述电子水印方法的步骤从而可以被计算机读出的存储介质。

由于涉及计算机网络的最新开发成果和可以得到廉价的高性能计算机，用于在网络上进行产品贸易的电子事务处理变得非常流行。用于这种事务的产品可以例如是包括图形的数字数据。

但是，由于可以很容易地制备数字数据的大量完整拷贝，所以，购买数字数据的用户将能够非法地制备具有与原件相同质量的拷贝然后分发所述拷贝数据。结果是，可被认为是正当的价格将不能付给具有数字数据版权的版权人或被版权人授权销售所述数字数据的个人（此后称为“销售者”），因此，将对所述版权产生侵害。

一旦版权人或销售者（此后将合法分发数字数据的个人称之为服务者）将数字数据传送给一个用户，则不可能对非法拷贝进行全面的保护。

因此，建议使用一种电子水印技术来代替直接避免非法拷贝的方法。根据这种电子水印技术，对原始的数字数据进行一个特殊的处理和涉及所述数字数据的版权信息、或用户信息被嵌入所述数字数据之间。由此，当发现所述数字数据的非法拷贝时，能够识别分发所述拷贝的个人。

在传统的电子水印系统中，假设服务者是完全可信赖的。因此，如果在传统系统中的一个服务者不可信赖和参加了某种非法分发活动，那么，一个没有犯罪的用户将被无辜地指控非法地拷贝了数据。

由于在图 1 所示的传统电子水印系统中，当一个服务者将用于识别所述用户的一个用户信息 d1 嵌入到数字数据 g（在下面的描述中，图象数据被作为数

字数据使用)中、且该用户信息 $d1$ 被分发给该用户和此后在没有征得该用户允许的情况下进一步分发含有该用户识别数据的数据时就会发生上述情况, 这样, 即使在这个例子中是服务者从事非法活动, 所述用户也没有办法反驳所述服务者的指控。

作为一种对策, 已经建议了一种图 2 所示的使用公共密钥加密法的系统。

根据这种公共密钥加密法, 加密密钥和解密密钥不同, 所述加密密钥被用做公共密钥, 而所述解密密钥被用做保密密钥。RSA 加密和 ElGamal 加密是典型的公知公共密钥加密系统的例子。

下面将对下述内容做出解释: (a) 公共密钥加密系统的特性; (b) 用于保密通信和验证通信的协议。

(a) 公共密钥加密的特性

(1) 由于加密密钥和解密密钥不同, 和由于所述加密密钥能够被公开, 所以, 所述加密密钥不需要保密传送处理并且它的分发是容易的。

(2) 由于用户的加密密钥是公开的, 所以, 用户仅仅需要提供他们解密密钥的保密存储。

(3) 可以提供一种验证功能, 利用该功能, 接收者能够验证一个消息的传送者没有欺骗行为和被接收的消息没有被改变。

(b) 用于公共密钥加密的协议

例如, 当 $E(kp, M)$ 表示用于使用公共加密密钥 kp 的消息 M 的加密操作, 和 $D(ks, M)$ 表示用于使用保密加密密钥 ks 的消息 M 的解密操作时, 公共密钥加密算法满足下述两个条件。

(1) 使用所提供的加密密钥 kp 可以很容易地执行加密 $E(kp, M)$ 的计算, 和使用所提供的解密密钥可以很容易地执行解密 $D(ks, M)$ 的计算。

(2) 只要用户不知道所述解密密钥 ks , 即使是该用户知道所述加密密钥 kp 和加密 $E(kp, M)$ 的计算方法和被加密的消息 $C = E(kp, M)$, 由于需要大量的计算, 所以, 该用户也不能够确定在消息 M 中包含甚麽内容。

除了条件 (1) 和 (2) 以外, 当下述条件 (3) 被满足时, 可以执行保密通信功能。

(3) 所述加密 $E(kp, M)$ 可以被规定用于所有消息 (明文) M , 从而建立

$$D(ks, E(kp, M)) = M$$

即,任何人都可以使用公共加密密钥 kp 执行用于加密 $E(kp, M)$ 的计算,但是,只有具有保密密钥 ks 的用户才能够执行用于解密处理 $D(ks, E(kp, M))$ 的计算以获得消息 M 的内容。

除了上述 (1) 和 (2) 以外,当满足下述条件 (4) 时可以执行验证通信。

(4) 所述解密处理 $D(ks, M)$ 可以被规定用于所有 (明文) 消息 M , 从而建立

$$E(kp, D(ks, M)) = M$$

即,只有具有保密解密密钥 ks 的用户才能够执行用于解密处理 $D(ks, M)$ 的计算。即使是其他的用户试图使用伪造的保密解密密钥 ks' 计算 $D(ks', M)$ 并执行应由具有所述保密解密密钥 ks 的用户进行的计算,所获得的结果也是

$$E(kp, D(ks', M)) \neq M,$$

接收者会了解所接收的信息是非法制备的。

当值 $D(ks, M)$ 被改变时,所获得的结果是

$$E(kp, D(ks, M)') \neq M$$

接收者会解所接收的信息是非法制备的。

在上述的加密方法中,使用公共加密密钥 (此后称之为公共密钥) 的操作 $E()$ 被称之为“加密”和使用保密解密密钥 (此后称之为保密密钥) 操作 $D()$ 被称之为“解密”。

因此,对于保密通信,传送者执行加密和接收者执行解密,而对于验证通信,传送者执行解密和接收者执行加密。

下面所示的协议被用于保密通信、验证通信、和用于具有由传送者 A 使用公共密钥加密系统附加的签名的接收者 B 的保密通信。

传送者 A 的保密密钥是 ksA 、公共密钥是 kpA , 和接收者 B 的保密密钥是 ksB 、公共密钥是 kpB 。

[保密通信]

以下过程是由传送者 A 向接收者 B 执行 (明文) 消息 M 的保密传送。

步骤 1: 传送者 A 向接收者 B 传送一个使用接收者 B 的公共密钥 kpB 以如下关系加密消息 M 所获得的一个消息 C :

$$C = E(kpB, M).$$

步骤 2: 为了获得原始明文消息 M , 接收者使用他或她的保密密钥 ksB 以如下关系解密所接收的消息 C :

$$M = E(k_{sB}, C).$$

由于接收者B的公共密钥 kp_B 对于很多未被规定的人来讲是可以公开得到的,所以,除所述传送者A之外的用户也能够将保密通信传送给所述接收者B.

[验证通信]

关于由传送者A向接收者B验证传送(明文)消息M,执行下述的处理

步骤1: 传送者A向接收者B传送通过使用他或她的保密密钥以如下关系建立的消息S:

$$S = D(k_{sA}, M).$$

这个消息S被称为被签名的消息,和用于制备这个被签名的消息的操作被称之为“签名”.

步骤2: 为了获得原始的明文消息M,接收者B使用传送者A的公共密钥 kp_A 将所述被签名消息S做如下转换:

$$M = E(k_{pA}, S).$$

如果接收者B确定消息M有意义,他或她验证所述消息M是由所述传送者A传送的.由于传送者A的公共密钥 kp_A 可以被很多未被规定的人得到,所以,除接收者B以外的用户也能够验证由所述传送者A传送的被签名的消息S.这个验证被称之为“数字签名”.

[具有签名的保密通信]

对由传送者A向接收者B保密传送已经被提供一个签名的(明文)消息M执行下述过程

步骤1: 传送者A使用他或她的保密密钥 ks_A 准备一个被签名的消息S以便以如下关系签名消息M:

$$S = D(k_{sA}, M).$$

此后,为了准备随后将要传送给接收者B的被加密的消息C,传送者A使用接收者B的公共密钥 kp_B 如下加密所述被签名的消息S:

$$C = E(k_{pB}, S).$$

步骤2: 为了获得被签名的消息S,接收者B使用他或她的保密密钥 ks_B 如下解密所述被解密的消息C:

$$S = D(k_{sB}, C).$$

然后,为了获得原始明文消息M,接收者B使用传送者A的公共密钥 kp_A 如下转换被签名的消息S:

$$M = E(kpA, S).$$

当接收者确定所述消息 M 有意义时, 他或她验证所述消息 M 是由所述传送者 A 传送的。

对于已经被提供签名的保密通信, 在各步骤执行计算功能的顺序可以被颠倒过来。换言之, 在上述的处理中, 以下述顺序执行下述步骤:

步骤 1: $C = E(kpB, D(ksA, M))$

步骤 2: $M = E(kpA, D(ksB, C))$ 。但是, 对于这种保密操作, 可以使用下述顺序:

步骤 1: $C = D(ksA, E(kpB, M))$

步骤 2: $M = D(ksB, D(kpA, C))$ 。

下面解释使用上述公共密钥加密方法的传统电子水印系统的操作过程。

1) 首先, 由服务者和用户准备一个涉及相互交换图象数据 g 的合同 $d2$ 。

2) 接着, 所述用户产生一个用于识别他或她本身的随机数 ID , 并使用这个 ID 产生一个单向函数 f 。

所述单向函数是一个当用于函数 $y = f(x)$ 时, 根据 x 计算 y 很容易, 但根据 y 计算 x 很困难的一个函数。例如, 用于具有一定数量位数的一个整数的唯一因数分解或离散对数被经常用做所述单向函数。

3) 然后, 用户使用他或她的保密密钥 ksU 准备被签名的信息 $d3$, 并利用所述合同 $d2$ 将它和单向函数 f 传送给服务者。

4) 此后, 服务者使用所述用户的公共密钥 kpU 验证被签名的信息 $D3$ 和合同 $d2$ 。

5) 在完成所述验证之后, 服务者将当前数据分发记录 $d4$ 和由用户准备的随机数 ID 嵌入所述图象数据 g 中, 并产生一个包括电子水印 ($g+d4+ID$) 的图象数据。

6) 最后, 服务者向所述用户传送包括电子水印 ($g+d4+ID$) 的图象数据。

当发现数据的非法拷贝时, 从所述非法图象数据中提取被嵌入的信息, 可以使用其中包括的 ID 识别一个特定的用户。此时, 服务者没有未经允许分发非法拷贝的声明是以下述根据为基础的。

由于用于规定一个用户的 ID 是由所述用户产生的, 和由于使用该 ID 将用户签名提供用于单向函数 f , 所以, 所述服务者能够不产生这样一个用于任一用户的 ID 。

但是，由于已经与所述服务者正式鉴定合同的用户必须将他或她的 ID 传送给所述服务者，因此，只有没有与所述服务者建立合同的用户不能被指控犯罪，而已经正式鉴定合同的用户能被指控犯罪。

因此，系统（图 3）已经被提出用于使已经正式鉴定合同的用户犯罪的指控不成立。

这个系统是通过将所述服务者分成原始图象服务者和嵌入服务者实现的。根据这个系统，在加密和解密期间，嵌入的电子水印不会被破坏。

下面解释图 3 所示系统的操作。

1) 首先，为了获得所希望的图象数据，用户发出一个将他或她的签名 d_5 加到原始图象服务者上的请求。

2) 所述原始图象服务者使用所述用户的签名 d_5 验证所述请求的内容，然后加密被请求的图象数据 g 并将被加密的数据传送给嵌入服务者。

此时，原始图象服务者向嵌入服务者传送一个带有与用户姓名 u 相关和与进行内容 d_6 相关的签名的图象数据。所述原始图象服务者还向所述用户传送一个与加密相关的解密函数 f' 。

3) 所述嵌入服务者验证所接收的加密图象数据 g' 和签名 $(u + d_6)$ ，并使用用户姓名 u 和进行内容 d_6 准备和嵌入用户信息 d_7 以用于具体地识别一个用户，并借此建立具有电子水印的加密数据 $(g' + d_7)$ 。然后，嵌入服务者向所述用户传送包括所述电子水印的加密图象数据 $(g' + d_7)$ 。

4) 用户使用从所述原始图象服务者接收的解密函数 f' 解密包括电子水印的加密图象数据 $(g' + d_7)$ ，并获得被提供有所述电子水印的图象数据 $(g + d_7)$ 。

当在以后发现非法拷贝时，原始图象服务者加密所述非法图象数据并提取被嵌入的信息，然后将该信息传送给嵌入服务者。嵌入服务者根据所述嵌入信息具体地识别一个用户。

在这个系统中，由于原始图象服务者没有在所述图象数据 g 中嵌入具体识别一个用户的用户信息 d_7 ，和由于嵌入服务者不了解所述解密函数 f （和不能够恢复所述原始图象），所以，单个的服务者不能非法地向正式订立合同的服务者分发被嵌入用户信息 d_7 的图象数据。

但是，在图 3 所示的系统中既没考虑到了原始图象服务者与嵌入服务者的串通，也没考虑到了嵌入服务者与用户的串通。由于嵌入服务者保持作为原始

00/08 00 15:43 FAX 00001000211848 NID DESIGN OFFICE 4002

图象数据的所述图象数据 g 的加密图象数据 g' ，和用户保持所述解密函数 f' ，所以当原始图象服务者与嵌入图象服务者串通时，图 2 所示的服务者可能执行一个非法活动。而当嵌入服务者与所述用户串通时，可能会非法获得所述原始图象（图象数据 g ）。

所述原始图象服务者将所述解密函数 f' 传送给所述用户，但是如果所述用户没有提供用于解密函数 f' 的适当管理控制，那么，即使是在所述嵌入服务者没有与所述用户串通的情况下，该用户的疏忽也将导致嵌入服务者获知所述解密函数。

另外，在图 3 所示的系统中，所述原始图象服务者没有包括嵌入装置，也不能使它正确地执行所述嵌入。但是，由于所述嵌入信息是由原始图象服务者提取的，所以，原始图象服务者能够通过分析所述嵌入信息正确地执行所述嵌入。

关于这个理由，由于所述嵌入服务者没有嵌入它自己的签名，所以，嵌入信息和用户信息之间的对应关系构成了唯一的嵌入服务者秘密。但是，嵌入信息和用户信息之间的对应关系并不是涉及数据库的使用的随机对应关系。如果根据一个特定规则从所述用户信息中准备所述嵌入信息，将有很大的可能性对所嵌入的信息进行分析。

在这种情况下，如图 2 的系统所示，执行一个非法活动是可能的。

另外，如上所述，当已经提出了包括用户和服务者的一个系统时，一个问题是不能保证利用分级提供服务者的系统所能够获得的保密性。

理由如下。例如，对于图 4 所示在服务者下配备了多个销售代理 1 到 m 并在单个销售代理下安排了用户 11 到 1 n 和用户 m 1 到 m n 的系统（分级网络 1）来讲，或者对于图 5 所示多个作者 1 到 m 中的一个作者请求代表他或她的销售代理销售他或她的图象数据和所述销售代理向多个用户 1 到 n 销售由相关作者编辑的图象数据的系统来讲，与数据贸易相关的参与组成部分从一个服务者和一个用户增加到一个服务者（或一个作者）、一个代理和一个用户，所以，在其中有三个参与组成部分的系统中发生的串通比起在有两个参与组成部分的系统中发生的更加复杂。

图 3 所示的系统可以被认为是包括一个服务者、一个代理和一个用户的系统。但是，传统的系统不是以分级系统为基础的，所述服务者是被分别提供的，以便避免可能由单个服务者执行的非法活动。如上所述，没有考虑到串通可能

发生。

为了克服上述缺陷，本发明的一个目的是提供一种即使是在执行所述数据贸易的组成部分是分级安排的情况下也能够精确避免数据非法分发的电子水印方法、电子信息分发系统、图象编档装置和存储媒体。

为了实现上述目的，根据本发明的一个方面，一种电子水印方法包括：

第一步骤，在该步骤中，第一实体执行与所述原始数据的第一加密处理；

第二步骤，在该步骤中，第二实体至少管理或分发由所述第一加密处理提供的数据和在所述数据中嵌入一个电子水印；和

第三步骤，在该步骤中，第三实体对已经被嵌入所述电子水印的数据执行第二加密处理。

根据本发明的另一个方面，用于在一个网络系统上交换数据的一个电子信息分发系统至少包括：

第一实体，包括第一加密装置，用于执行所述原始数据的第一加密处理；

第二实体，包括用于至少管理或分发由所述第一加密处理提供的数据的管理分发装置，并包括用于在所述数据中嵌入一个电子水印的电子水印嵌入装置；和

第三实体，包括用于对已经嵌入所述电子水印的数据进行第二加密的第二加密装置。

根据本发明的再一个方面，一个电子水印方法包括如下步骤：

使用多个装置或实体执行用于加密和用于一个电子水印嵌入的分发处理；和

使用附加装置或实体检查至少是所述加密处理或用于由所述多个装置或实体执行的嵌入电子水印的处理的合法性。

这些装置或实体可以至少由三种装置或实体组成。

根据本发明的另一个附加方面，用于在由多个实体构成的一个网络系统上交换数据的电子水印分发系统包括：

第一实体，包括第一数据加密装置；

第二实体，包括电子水印嵌入装置，用于管理和分发从所述第一实体接收的数据的；

第三实体，包括第二加密装置，用于使用已经被嵌入所述电子水印的数据的；和

第四实体, 用于检查至少是所述加密处理或由所述第一到第三实体执行的电子水印嵌入处理的合法性。

根据本发明的再一个方面, 用于在由多个实体构成的一个网络系统上交换数据的电子信息分发系统包括:

第一实体, 包括第一数据加密装置;

第二实体, 包括电子水印嵌入装置, 用于管理和分发从所述第一实体接收的数据;

第三实体, 包括一个电子水印嵌入装置和第二加密装置, 用于使用其中已经被嵌入一个电子水印的数据; 和

第四实体, 用于检查至少由所述第一到第三实体执行的所述加密处理或电子水印嵌入处理的合法性。

根据本发明的再一个方面, 用于在由多个实体构成的一个网络上交换数据的电子信息分发系统包括:

第一实体, 包括一个电子水印嵌入装置和第一数据加密装置;

第二实体, 包括电子水印嵌入装置, 用于管理和分发从所述第一实体接收的数据;

第三实体, 包括第二加密装置, 用于使用其中已经被嵌入一个电子水印的数据;

第四实体, 用于检查至少由所述第一到第三实体执行的所述加密处理或所述电子水印嵌入处理的合法性。

根据本发明的再一个方面, 用于在由多个实体构成的网络系统上交换数据的电子信息分发系统包括:

第一实体, 包括一个电子水印嵌入装置和第一加密装置;

第二实体, 包括电子水印嵌入装置、第一加密装置和第二加密装置中的至少一个, 用于管理和分发从所述第一实体中接收的数据;

第三实体, 包括电子水印嵌入装置和第二加密装置, 用于使用其中已经被嵌入一个电子水印的数据; 和

第四实体, 用于检查至少由第一到第三实体执行的所述加密处理或所述电子水印嵌入处理的合法性。

根据本发明的另一个方面, 一种电子水印叠加方法包括如下步骤:

加密电子信息和交换所生成的电子信息;

在加密处理期间在所述电子水印中嵌入一个电子水印信息; 和
重复多次用于传送具有一个电子水印的电子信息的处理,
借此, 第一实体传送其上已经被叠加有所述电子水印信息的电子信息并经过第二实体传送给第三实体。

根据本发明的再一个方面, 一个电子信息分发系统包括:

保持有原始电子信息的第一实体, 包括用于加密所述原始电子信息的加密装置和用于在由所述加密处理提供的电子信息中嵌入一个电子水印的嵌入装置;

第二实体, 包括用于管理和分发从所述第一实体接收的电子信息 and 加密所述信息的加密装置, 和包括用于在所述电子信息中嵌入一个电子水印信息的嵌入装置; 和

第三实体, 包括用于加密从所述第二实体接收的电子信息的加密装置, 用于使用所生成的电子信息。

根据本发明的再一个方面, 提供了一种电子水印叠加方法, 借此用于由一个传送实体向接收实体传送电子信息, 所述传送实体对已经由所述接收实体加密的电子信息重复执行电子水印处理, 以便由第一实体经过第二实体向第三实体至少传送已经被叠加了一个电子水印的电子信息。

根据本发明的再一个方面, 一种电子水印叠加方法包括如下步骤:

传送实体执行对电子信息的第一加密处理:

接收实体对所生成的电子信息执行不同于所述第一加密处理的第二加密处理, 和将所获得的电子信息返回给传送实体; 和

传送实体解密已经被执行了第一加密处理的电子信息和在已经被解密的电子信息中嵌入电子水印信息,

借此, 通过重复上述步骤, 所述第一实体经过第二实体向第三实体至少传送其上已经被叠加有所述电子水印信息的电子信息。

根据本发明的再一个方面, 一个电子信息分发系统包括:

第一实体, 其上保持有所述原始电子信息;

第二实体, 用于管理和分发从所述第一实体接收的电子信息; 和

第三实体, 用于使用从所述第二实体接收的所述电子信息,

其中, 为了从传送实体向接收实体传送电子信息, 所述传送实体重复用于在电子信息中嵌入一个电子水印的处理, 以便从所述第一实体经过第二实体向

第三实体至少传送其中已经被嵌入电子水印信息的电子信息。

根据本发明再一个方面，一个电子信息分发系统包括：

第一实体，上面保持有原始电子信息；

第二实体，用于管理和分发从所述第一实体接收的电子信息；和

第三实体，用于使用从所述第二实体接收的所述电子信息，

其中，接收实体对已经被传送实体执行了不同于第二加密处理的第一加密处理的电子信息执行第二加密处理，和将所生成的电子信息返回给所述传送实体，

其中，传送实体解密已经被执行第一加密处理的电子信息并在所生成的电子信息中嵌入所述电子水印信息，和

其中通过重复所述处理，所述第一实体经过第二实体向第三实体至少传送其上已经被叠加了电子水印信息的电子信息。

图 1 用于解释传统的电子水印系统；

图 2 用于解释通过改善图 1 所示系统获得的传统电子水印系统 (1)；

图 3 用于解释通过改善图 1 所示系统获得的传统电子水印系统 (2)；

图 4 用于解释使用传统电子水印方法的分级系统 (包括一个服务者、代理和多个用户)；

图 5 用于解释使用传统电子水印方法的分级系统 (包括多个作者、代理和多个用户)；

图 6 的框图示出了根据本发明第一实施例一个系统的配置；

图 7 的流程用于解释由所述系统执行的验证处理；

图 8 的框图示出了根据本发明第二实施例一个系统的配置；

图 9 的框图示出了根据本发明第三实施例一个系统的配置；

图 10 用于解释一般的图象格式；

图 11 用于解释图象文件结构 (I)；

图 12 用于解释图象文件结构 (II)；

图 13 用于解释用于存储图象数据的方法的属性；

图 14 用于解释由多个具有不同分辨率的图象构成的图象文件的例子；

图 15 用于解释在具有不同分辨率的层上的图象；

图 16 用于解释各图象数据的铺砌数据；

图 17 用于解释根据本发明第四实施例的一个电子水印系统；

图 18 用于解释根据本发明第五实施例的一个电子水印系统;
图 19 用于解释根据本发明第六实施例的一个电子水印系统;
图 20 用于解释根据本发明第七实施例的一个电子水印系统;
图 21 用于解释根据本发明第八实施例的一个电子水印系统;
图 22 示出了根据本发明第九实施例到第十二实施例的系统结构;
图 23 的框图用于解释第九实施例;
图 24 的框图用于解释第十实施例;
图 25 的框图用于解释第十一实施例; 和
图 26 的框图用于解释第十二实施例。

下面参照附图描述本发明的最佳实施例。

(第一实施例)

本发明被用于例如图 4 所示的分级系统(该系统包括多个代理)。

图 6 简要示出了图 4 所示系统的由一个服务者、多个代理和属于该代理的多个用户构成的配置。

参考图 6 将具体地解释系统 100。

系统 100 是一个网络系统,它是由多个实体(未示出)构成的,所述实体包括位于服务者一侧的终端 10(服务者终端)、位于代理一侧的终端 40(代理终端)和位于用户一侧的终端 20(用户终端)。各个实体在所述网络上交换数字数据。

服务者终端 10 包括: 合同识别单元 11, 用于从所述用户终端 20 接收数据; 电子水印嵌入单元 12, 用于接收例如图象数据(数字数据)G 和代理信息 M; 第一加密单元 13, 用于接收电子水印嵌入单元 12 的输出; 第一解密单元, 用于从所述代理终端 40 接收数据; 和识别单元 15, 用于从代理终端 40 接收数据; 和散列发生器 16, 用于接收第一解密单元 14 的输出。

第一解密单元 14 和散列发生器 16 的输出被传送给代理终端 40, 第一解密单元 14 的输出经过代理终端 40 被传送给散列发生器 16 和用户终端 20。

所述代理终端 40 包括: 合同发生器 41, 用于从所述用户终端 20 接收数据; 电子水印嵌入单元 42, 用于接收合同发生器 41 和所述服务者终端 10 的第一加密单元 13 的输出; 第三解密单元, 用于接收电子水印嵌入单元 42 的输出; 散列发生器 44, 用于接收第三加密单元 43 的输出; 识别单元 45, 用于接收所述散列发生器 44 的输出; 第三解密单元 46 和识别单元 47, 用于从所述用户终

端 20 接收数据; 和电子水印嵌入单元 48, 用于接收第三解密单元 46 的输出。

从第三加密单元 43 输出的数据被传送给散列发生器 44, 还被传送给服务者终端 10 的第一解密单元 14 和识别单元 15。从服务者终端 10 的散列发生器 16 输出的数据也被传送给识别单元 45, 从所述识别单元 45 输出的数据也被传送给用户终端 20。另外, 来自用户终端 20 的数据被传送给电子水印嵌入单元 48, 和从该电子水印嵌入单元 48 输出的数据被传送给用户终端 20。

所述用户终端 20 包括: 合同发生器 21, 用于将数据传送给所述代理终端 40 的合同识别单元 41; 第二加密单元 24 和识别/签名发生单元 28, 用于经过所述代理终端 40 从服务者终端 10 的第一解密单元 14 接收数据; 散列发生器 26, 用于从第二加密单元 24 接收数据; 和第二解密单元 27, 用于接收所述代理终端 40 的电子水印嵌入单元 48 的输出。

由所述第二解密单元 24 产生的数据被传送给散列发生器 26, 并传送给所述代理终端 40 的第三解密单元 46 和识别单元 47。由散列发生器 26 产生的数据也被输出给代理终端的识别单元 47。由所述代理终端 40 的识别单元 45 产生的数据被传送给识别/签名发生单元 28。

在上述的系统 100 中, 涉及诸如所使用方法和保密密钥的的第一加密处理的信息仅仅是所述服务者可以得到的信息; 涉及第二加密处理的信息仅仅是所述用户可以得到的信息; 和涉及第三加密处理的信息仅仅是所述代理可以得到的信息。

但是, 应当说明, 这些加密处理的特性是没有考虑首先执行哪一个加密处理, 使用解密处理可以译码一个消息。

下面, 利用 “ $E_i()$ ” 表示加密处理, 利用 “ $D_i()$ ” 表示解密处理和利用 “+.” 表示涉及电子水印的嵌入处理。

由此, 下面将首先解释由系统 100 执行的电子水印嵌入处理。

[嵌入处理]

1) 首先, 为了获得所希望的图象数据, 用户终端 20 向所述代理发出一个具有所述用户签名的请求。被请求的数据是由所述合同发生器 21 产生的信息 (用户签名信息), 该信息此后被称之为合同信息。

代理终端 40 从所述用户接收合同信息, 识别该信息并请求服务者提供该图象数据。

2) 服务者终端 10 的电子水印嵌入单元 12 在从所述代理接收的图象数据 G

中嵌入代理信息 M。

第一加密单元 13 对其中已经由所述电子水印嵌入单元 12 嵌入所述代理信息 M 的图象数据 (G+M) 执行第一加密 $E()$ ，并且将所生成的图象数据传送给所述代理。

在这个方式下，代理终端 40 接收第一被加密图象数据 $E1(G+M)$ 。

3) 代理终端 40 的合同发生器 41 使用与所述用户相关的合同信息产生用户信息 U。

电子水印嵌入单元 42 在从所述服务者接收的第一被加密图象数据 $E1(G+M)$ 中嵌入由所述合同发生器 41 产生的用户信息 U。

第三加密单元 43 对其中已经由所述电子水印嵌入单元 42 嵌入了用户信息 U 的第一被加密图象数据 $E1(G+M)+U$ 执行第三加密处理 $E3()$ ，并将所获得的图象数据 (第三被加密数据) $E3(E1(G+M)+U)$ 传送给所述服务者。

在此同时，散列发生器 44 产生用于传送数据 (第三被加密图象数据) $E3(E1(G+M)+U)$ 的散列值 H1、对它签名和将所获得的散列值 H1 传送给服务者终端 10。

结果是，服务者终端 10 利用它的签名接收第三被加密图象数据 $E3(E1(G+M)+U)$ 和散列值 H1。

所述散列值是一个通过计算所述散列函数 $h()$ 获得的一个值，所述散列函数是一个很少引起冲突的压缩函数。在这种情况下冲突意味着对于不同值 $x1$ 和 $x2$ 来讲， $h(x1) = h(x2)$ 。所述压缩函数是一个用于将具有特定位长的位串转换成具有不同位长的位串的函数。因此，所述散列函数是这样一个函数，即利用该函数将具有一个特定位长的位串转换成具有不同位长的位串，和对于这个函数，不容易发现满足 $h(x1) = h(x2)$ 的值 $x1$ 和 $x2$ 。由于不容易从一个任意值 y 中获得满足 $y = h(x)$ 的值 x ，因此，散列函数是一个单向函数。关于所述散列函数的例子是 MD (消息摘要) 5 或 SHA (保密散列算法)。

4) 服务者终端 10 的识别单元 15 识别与从所述代理终端 40 接收的散列值 H1 相关的签名，并确认所述散列值与使用所述传送数据 (第三被加密图象数据) $E3(E1(G+M)+U)$ 产生的一个散列相匹配。在完成所述确认处理之后，识别单元 15 存储所接收的数据。

第一解密单元 14 解密从代理终端 40 接收的所述第三加密图象数据 $E3(E1$

(G+M)+U) 的第一加密部分, 并将所获得的图象数据传送给用户终端 20.

在此同时, 散列发生器 16 产生散列值 H2, 用于传送数据 E3 (G+M+D1 (U))、对它签名和将所述数据传送给代理终端 40.

因此, 代理终端 40 利用它的签名接收数据 E3 (G+M+D1 (U)).

5) 代理终端 40 的识别单元 45 识别与从服务器终端 10 接收的散列值 H2 相关的签名, 确认所述散列值 H2 与用于传送数据 E3 (G+M+D2 (U)) 的散列值相匹配. 在完成所述确认处理之后, 识别单元 45 存储所接收的数据.

另外, 识别单元 45 将从所述服务器接收的数据传送给没有变化的用户.

因此, 用户终端 20 利用它的签名接收数据 E3 (G+M+D1 (U)) 和散列值 H2.

6) 识别/签名发生单元 28 识别与从代理终端 40 接收的散列值 H2 相关的签名, 确认所述散列值 H2 与用于传送数据 E3 (G+M+D1 (U)) 的散列值相匹配. 在完成所述确认处理之后, 存储所接收的数据.

另外, 所述识别/签名发生单元 28 产生它自己的用于所述散列值 H2 的签名 A, 并利用该签名将所述散列值 H2 经过所述代理传送给所述服务器.

代理终端 40 的识别单元 45 和服务终端 10 的散列发生器 16 识别由所述用户传送的签名 A 然后存储它.

7) 用户终端 20 的第二加密单元 24 对从所述代理接收的数据 E3 (G+M+D1 (U)) 执行第二加密处理 E(), 并将获得的数据传送给所述代理.

在此同时, 散列发生器 26 产生散列值 H3, 用于传送所述数据 E2 (E3 (G+M+D1 (U)))、对它签名并利用所述签名传送散列值 H3 给所述代理. 另外, 散列发生器 26 产生它自己的认证数据 S 并将该数据传送给所述代理.

结果是, 代理终端 40 利用它的签名接收数据 E2 (E3 (G+M+D1 (U))) 和散列值 H3 以及所述认证信息 S.

8) 代理终端 40 的识别单元 47 识别与从所述用户接收的散列值 H3 相关的所述签名, 并确认所述散列值 H3 与用于传送数据 E2 (E3 (G+M+D1 (U))) 的散列值相匹配. 在完成所述确认处理之后, 存储所接收的数据.

第三解密单元 46 解密从所述用户接收的数据 E2 (E3 (G+M+D1 (U))) 的第三被加密部分.

电子水印嵌入单元 48 在通过第三解密单元 46 获得的数据 E2 (G+M+D1 (U)) 中嵌入所述认证信息 S, 并将所生成的数据 E2 (G+M+D1 (U)) + S 传

送给所述用户。

散列发生器 49 产生一个用于数据 $E2(G+M+D1(U))$ 的散列值 $H4$ ，对它签名和将生成的散列值 $H4$ 传送给所述用户。

在这种方式下，用户终端 20 接收数据 $E2(G+M+D1(U))+S$ 。

9) 用户终端 20 的识别单元 29 识别与从所述代理接收的散列值 $H4$ 相关的签名，和确认所述散列值 $H4$ 与用于传送数据 $E2(G+M+D1(U))$ 的散列值相匹配。在完成该确认处理之后，存储所接收的数据。第二解密单元 27 解密数据 $E2(G+M+D1(U))+S$ 的第二加密部分，并利用所述电子水印提取和输出图象数据 G 。

图象数据 G 被表示为：

$$G_s = G + M + D1(U) + D2(S)。$$

这指出代理信息 M 、第一被加密用户信息（电子水印信息）和第二加密签名信息 S 被嵌入到所述原始图象数据中。

如上所述，由于所述代理负责嵌入与所述用户相关的签名信息，所以，所述用户基本不会执行非法活动。当所述代理嵌入用户信息 U 和与所述用户相关的签名信息 S 时，所述用户信息 U 受只有所述服务者了解的第一加密的影响，而签名信息受只有所述用户了解的第二加密的影响。因此，所述代理不能够在原始图象数据 G 中直接嵌入数据 $D1(U+D2(S))$ 。

当发现非法拷贝（非法图象）时，通过执行图 2 所示的处理（以后该处理被称之为验证处理）规定非法用户。但是，在这个实施例中，应当说明所述图象数据不受电子水印信息的修改或删除的影响。

[验证处理]

1) 首先，所述服务者终端 10 从所发现的非法图象 G_s' 中提取代理信息 M' （步骤 S101）。

当代理信息 M' 没有被提取时，它确定所述服务者（或作者）进行了一个非法活动（步骤 A102）。这是由于服务者一侧在所述图象数据中嵌入了所述代理信息 M' 。

2) 当在 1) 正确地提取了所述代理信息 $M(M=M')$ 时，所述服务者向所述验证办公室 30 提供所述非法的图象数据 G_s' 和所述第一加密密钥，并请求第一加密所述非法图象数据 G_s' （步骤 S103）和提取用户信息 U' （步骤 S104）。

当正确的用户信息 U' 被提取（ $U=U'$ ）时，程序控制前进到 8），该处

理将在下面描述。

3) 当在 2) 没有提取正确的用户信息时, 验证办公室 30 利用它自己的签名请求来自服务者存储数据 $E3(E1(G+M)+U)$ 和所述散列值 $H1$ 。然后验证办公室 30 解密数据 $E3(E1(G+M)+U)$ 的第一被加密部分, 产生它的散列值, 和确认那个散列值与由所述代理存储的散列值 $H2$ 相匹配。与此同时, 验证办公室 30 检查提供给散列值 $H2$ 的签名 (步骤 S105)。

4) 当在 3) 由所述验证办公室 30 产生的散列值 $H1$ 与由所述代理存储的散列值 $H2$ 不相匹配时, 验证办公室 30 确定进行了非法活动的服务者 (步骤 S106)。

这意味着由所述服务者提供的所述第一加密是不正确的。

5) 当在 3) 由所述验证办公室 30 产生的散列值与由所述代理存储的散列值 $H2$ 相匹配时, 验证办公室 30 请求所述代理提供第三加密密钥, 解密由所述服务者存储的数据 $E3(E1(G+M)+U)$ 的第三加密部分, 并从所获得的数据中提取所述用户信息 U' (步骤 S107)。

6) 当在 5) 提取到了正确的用户信息 U' 时 ($U'=U$), 验证办公室 30 确定进行了非法活动的服务者 (步骤 S108)。

这指出用户信息 U' 已经被正确地嵌入到所述图象数据中。另外, 由于经过直到 5) 的验证处理, 所以它确定与所述非法图象数据 G' 相关的第一被加密部分是非法的, 很明显, 只有了解所述第一加密密钥的服务者才能够产生所述非法的图象数据 G' 。

7) 当在 5) 没有提取正确的用户信息 U' 时, 验证信息 30 确定进行了非法活动的代理 (步骤 S109)。

这指出在嵌入处理期间在所述图象数据中没有嵌入正确的一个信息 U' , 和所述代理曾经负责嵌入所述用户信息。

8) 当在 2) 提取了正确的用户信息 U' ($U'=U$) 时, 验证办公室 30 请求服务者和代理提供所存储的散列值 $H2$ 和由与所述散列值 $H2$ 相关的用户提供的签名 A' (步骤 S110)。

9) 当在 8) 没有识别出 (没有提供) 所述正确的签名 A' 时, 验证办公室 30 确定所述服务者和代理串通进行非法活动 (步骤 S111)。

这指出所述服务者和代理串通伪造代表任一用户 (用户信息 U') 的数据 $G+M+D1(U')$ 。

10) 当在 8) 识别出正确的签名 A' ($A' = A$) 时, 验证办公室 30 请求所述用户提供第二加密密钥, 并执行与所述非法图象数据 G' 相关的第二加密(步骤 S112)。然后, 提取所述签名信息 S' (步骤 S113)。

11) 当在 10) 提取到所述正确的签名信息 S' ($S' = S$) 时, 验证办公室 20 确定所述用户进行了一个非法活动(步骤 S114)。

这是由于用于执行第二加密处理和用于提取签名信息 S' 的处理可以只由所述用户执行。

12) 当在 10) 没有能够提取正确的签名信息 S' 时, 验证办公室 30 利用它的签名请求所述用户提供所存储的图象 $E3(G+M+D1(U))$ 、散列值 $H3$, 并识别所述散列值 $H3$ 和所述签名。然后, 验证办公室 30 对数据 $E3(G+M+D1(U))$ 执行第二加密, 和产生与所述数据相关的散列值, 以便确定它是否与所述散列值 $H3$ 相匹配。与此同时, 验证办公室 30 还检查与所述散列值 $H3$ 相关的签名(步骤 S115)。

13) 当在 12) 由所述验证办公室 30 产生的散列值与用户所存储的散列值 $H3$ 不相匹配时, 验证办公室 30 确定所述用户进行了一个非法活动(步骤 S116)。

这是由于由所述用户提供的第二加密密钥是不正确的。

14) 当在 12) 由验证办公室 30 产生的散列值与由所述用户存储的散列值 $H3$ 相匹配时, 验证办公室 30 确定已经由所述用户进行了一个非法活动(步骤 S117)。

这是由于在所述嵌入处理期间所述代理确实没有在所述图象数据中嵌入正确的签名信息 S 。

如上所述, 根据本实施例, 在发现一个非法活动之前并不需要所述的验证办公室, 和在发现一个非法活动之前不能确定执行了任何非法活动。另外, 只要上述验证处理是已知的, 和所述服务者、所述代理和所述用户监视那个处理的结果, 那么, 即使是包括所述验证办公室 30, 也可以根据所述情况规定由它们执行的非法活动。

(第二实施例)

本发明例如可以被应用于图 5 所示的分级系统(只包括一个代理的系统)。

图 8 简要地示出了例如图 5 所示多个作者(或服务者)、一个代理和任一

用户之一或多个用户之一的配置。

下面将结合图 8 详细解释系统 200。

除了下面的区别以外，系统 200 与图 6 所示系统 100 具有相同的结构：

1) 在服务者终端 10 中没有提供电子水印嵌入单元 12，和只有图象数据 G 被传送给第一加密单元 13。

2) 还提供了—个用于代理终端 40 并用于接收电子水印嵌入单元 48 输出的散列发生器 49。由所述散列发生器 49 产生的数据被传送给用户终端 20。

3) 识别单元 29 被附加提供给用户终端 20 并接收代理终端 40 中电子水印嵌入单元 48 和散列发生器的输出。

如上所述，系统 200 被设计成省略嵌入表示一个代理的代理信息 M。

首先，将解释由所述系统 200 执行的电子水印嵌入处理。

使用与图 6 中的系统 100 所使用相同的标号表示图 8 所述系统 200 中的相应部分，下面将给出相关部分的详细解释。

[嵌入处理]

1) 首先，为了获得图象数据（合同信息），用户终端 20 向所述代理发出具有该用户的签名的请求。

代理终端 40 接收来自该用户的合同信息，识别它并且请求服务者提供该图象数据。

2) 在所述服务者终端 10 中，第一加密单元 13 对图象数据 G 执行第一加密处理 E1，并将所生成的图象数据传送给所述代理。

在这种方式下，代理终端 40 接收第一被加密图象数据 E1 (G)。

3) 代理终端 40 的合同发生器 41 使用与所述用户相关的合同信息产生用户信息 U。

电子水印嵌入单元 42 在从所述接收的第一被加密图象数据 E1 (G) 中嵌入由所述合同发生器 41 产生的用户信息 U。

第三加密单元 43 对其中已经由所述电子水印嵌入单元 42 嵌入所述用户信息 U 的第一被加密图象数据 E1 (G) + U 执行第三加密处理 E3，并将所获得的图象数据（第三被加密图象数据）E3 (E1 (G) + U) 传送给所述服务者。

与此同时，散列发生器 44 产生用于所述传送数据（第三被加密图象数据）E3 (E1 (G) + U) 的散列值 H1，对它签名和将所获得的散列值 H1 传送给服务者终端 10。

结果是, 服务者终端 10 利用它的签名接收第三被加密图象数据 $E3(E1(G) + U)$ 和所述散列值 $H1$ 。

4) 服务者终端 10 的识别单元 15 识别用于从所述代理终端 40 接收的所述散列值 $H1$ 的签名, 并确认散列值 $H1$ 与使用所述传送数据 (第三被加密图象数据 $E3(E1(G) + U)$) 产生的一个散列值相匹配。在完成所述确认处理之后, 识别单元 15 存储所接收的数据。

第一解密单元 14 解密从所述代理终端 40 接收的第三被加密图象数据 $E3(E1(G) + U)$ 的第一被加密部分, 并将所获得的图象数据传送给所述用户终端 20。

与此同时, 散列发生器 16 产生用于所述传送数据 ($E3(G + D1(U))$) 的散列值 $H2$ 、对它签名和将所述数据传送给代理终端 40。

由此, 代理终端 40 利用它的签名接收数据 $E3(G + D1(U))$ 和散列值 $H2$ 。

5) 代理终端 40 的识别单元 45 识别用于从服务者终端 10 接收的散列值 $H2$ 的签名, 确认散列值 $H2$ 与用于传送数据 $E3(G + D1(U))$ 的散列值相匹配。在完成所述确认处理之后, 识别单元存储所接收的数据。

另外, 识别单元 45 将从所述服务者接收的数据传送给没有变化的所述用户。

因此, 用户终端 20 利用它的签名接收数据 $E3(G + D1(U))$ 和散列值 $H2$ 。

6) 识别/签名发生单元 28 识别用于从代理终端 40 接收的散列值 $H2$ 的签名, 确认所述散列值 $H2$ 与用于所述传送数据 $E3(G + D1(U))$ 的散列值相匹配。在完成所述确认处理之后, 存储所接收的数据。

另外, 识别/签名发生单元 28 产生它自己的用于散列值 $H2$ 的签名 A , 并利用这个签名将散列值 $H2$ 经过所述代理传送给所述服务者。

代理终端 40 的识别单元 45 和服务者终端 10 的散列发生器 16 识别由所述用户传送的签名 A , 然后存储它。

7) 用户终端 20 的第二加密单元 24 对从所述代理接收的数据 $E3(G + D1(U))$ 执行第二加密处理 $E()$, 并将获得的数据传送给所述代理。

与此同时, 散列发生器 26 产生用于传送数据 $E2(E3(G + D1(U)))$ 的散列值 $H3$ 、对它签名并利用该签名将所述散列值 $H3$ 传送给所述代理。另外, 散列发生器 26 产生它自己的验证数据 S , 并将它传送给所述代理。

结果是, 代理终端 40 利用它的签名接收数据 $E2(E3(G + D1(U)))$, 散列 H3 和验证信息 S.

8) 代理终端 40 的识别单元 47 识别用于从所述用户接收的散列值 H3 的签名, 并确认所述散列值 H3 与用于所述传送数据 $E2(E3(G + D1(U)))$ 的散列值相匹配. 在所述确认处理完成之后, 存储所接收的数据.

第三解密单元 46 解密从所述用户接收的数据 $E2(E3(G + D1(U)))$ 的第三被加密部分.

电子水印嵌入单元 48 将所述验证信息 S 嵌入到通过第三解密单元 46 获得的数据 $E2(G + D1(U))$ 中, 并将生成的数据 $E3(G + D1(U)) + S$ 传送给所述用户.

在这种方式下, 用户终端 20 接收数据 $E2(G + D1(U)) + S$.

9) 在用户终端 20 中, 第二解密单元 27 解密数据 $E2(G + D1(U)) + S$ 的第二被加密部分, 利用一个电子水印提取并输出图象数据 G_u .

所述图象数据 G_u 被表示为:

$$G_u = G + D1(U) + D2(S).$$

这指出第一被加密用户信息 (电子水印信息) U 和第二被加密签名信息 S 被嵌入到所述原始图象数据中.

如上所述, 由于所述代理负责嵌入用于所述用户的签名信息, 所述用户基本上不能执行非法活动. 当代理嵌入用于所述用户的用户信息 U 和签名信息 S 时, 所述用户信息 U 受只有所述服务者了解的第一加密的影响, 而所述签名信息 S 受只有所述用户了解的第二加密的影响. 因此, 所述代理不能在原始数据 G 中直接嵌入 $D1(U + D2(S))$.

当发现一个非法拷贝 (非法活动) 时, 通过执行下述的验证处理不必使用上述的代理信息 M 就能够确定进行非法活动的代理. 应当说明, 图象数据是不受电子水印的修改和删除影响的.

[验证处理]

1) 首先, 所述服务者向验证办公室 30 提供从已经被发现的非法图象数据 G_u' 获得的第一加密密钥, 并请求所述非法图象数据 G_u' 的第一加密和提取用户信息 U' .

当提取了正确的用户信息 U' ($U' = U$) 时, 程序控制前进到 7), 这将在下面解释.

2) 当在 1) 没有提取到正确的用户信息时, 验证办公室 30 利用它的签名向服务者请求所存储的数据 $E3(E1(G)+U)$ 和散列值 $H1$ 。然后, 验证办公室 30 识别所述散列值 $H1$ 和所述签名。此后, 验证办公室 30 解密数据 $E3(E1(G)+U)$ 的第一被加密部分, 产生它的散列值, 并确认所述散列值与所述代理存储的散列值 $H2$ 相匹配。与此同时, 验证办公室 30 检查用于散列值 $H2$ 的签名。

3) 当在 2) 由所述验证办公室 30 产生的散列值与由所述代理存储的散列值 $H2$ 相互不匹配时, 验证办公室 30 确定进行了一个非法活动的服务者。

这意味着由所述服务者提供的第一加密密钥是不正确的。

4) 当在 2) 由所述验证办公室 30 产生的散列值与由所述代理存储的散列值 $H2$ 相互匹配时, 验证办公室 30 请求所述代理提供第三加密密钥, 解密由所述服务者存储的根据 $E3(E1(G)+U)$ 的第三加密部分, 并从所获得的数据中提取用户信息 U' 。

5) 当在 4) 提取到了正确的用户信息 U' ($U' = U$) 时, 验证办公室 30 确定进行了一个非法活动的服务者。

这指出在所述图数据中已经正确地嵌入了用户信息 U' 。另外, 由于经过直到 4) 的验证处理已经确定用于所述非法图象数据 G' 的第一被加密部分是正确的和所述用户信息 U' 是非法的, 所以, 很明显, 只有了解第一加密密钥的服务者才能够产生非法的图象数据 G' 。

6) 当在 4) 没有提取到正确的用户信息 U' 时, 验证办公室 30 确定进行了非法活动的代理。

这指出在嵌入处理期间没有与所述图象数据中嵌入正确的用户信息 U' , 和所述代理曾经负责嵌入所述用户信息。

7) 当在 1) 提取到了正确的用户信息 U' ($U' = U$) 时, 验证办公室 30 请求所述用户和代理提供所存储的散列值 $H2$ 和由所述用户为所述散列值 $H2$ 提供的签名 A' , 并识别所述签名 A' 。

8) 当在 7) 没有提取到正确的用户信息 A' (没有提供) 时, 验证办公室 30 确定所述服务者和代理串通一个非法活动。

这指出所述服务者和代理串通伪造表示任一用户的数据 $G+D1(U')$ (用户信息 U')。

9) 当在 7) 识别出所述正确的签名 A' ($A' = A$) 时, 验证办公室 30 请求所述用户提供第二加密密钥, 并对非法图象数据 G' 执行第二加密。然后, 提

取签名信息 S' 。

10) 当在 9) 提取到正确的签名信息 S' ($S' = S$) 时, 验证办公室 20 确定所述用户进行了非法活动。

这是由于用于执行第二加密处理和用于提取所述签名信息 S' 的处理可以只由所述用户来执行。

11) 当在 9) 没有提取到所述正确的签名信息 S' 时, 验证办公室 30 利用它的签名请求所述用户提供所存储的图象 $E3(G + D1(U))$ 和散列值 $H3$, 并识别所述散列值 $H3$ 和所述签名。然后, 验证办公室 30 对数据 $E3(G + D1(U))$ 执行第二加密处理并产生一个与所述数据相关的散列值以便确定它是否与散列值 $H3$ 相匹配。与此同时, 验证办公室 30 还检查用于散列值 $H3$ 的签名。

12) 当在 11) 由所述验证办公室 30 产生的散列值与由所述用户存储的散列值 $H3$ 不相匹配时, 验证办公室 30 确定所述用户进行了一个非法活动。

这是由于由所述用户提供的第二加密密钥是不正确的。

13) 当在 11) 由所述验证办公室 30 产生的散列值与由所述用户存储的散列值 $H3$ 相互匹配时, 验证办公室 30 确定由所述代理进行了一个非法的活动。

这是由于在所述嵌入处理期间所述代理没有在所述图象数据中嵌入正确的签名信息 S 。

如上所述, 根据该第二实施例, 在发现非法图象之前不需要所述验证办公室, 并且在发现一个非法图象数据之前, 不能确定已经执行了任何一个非法活动。另外, 只要上述验证处理是已知的和所述服务者、代理以及用户监视那个处理的结果, 即使是没有包括所述验证办公室 30, 也能够根据所述签名规定由它们进行的非法活动。

(第三实施例)

最近, 已经开始在一个网络的上进行货币传输, 即被称之为电子现金的资金传送处理。由于按照一般的现金交付方法, 对所述电子现金传送拥有者的姓名不进行识别, 所以, 必须获得一个匿名。如果不可能获得所述的匿名, 那么, 一个产品的销售者应当从一个涉及其产品的购买者和使用的电子现金传送信息中获得该匿名, 所述用户的秘密将得不到保护。因此, 对用户秘密的保护和为授权使用一个电子水印的创建者的版权所提供的保护是一样重要的。

因此, 在第三实施例中, 必须为购买者提供一个用户的匿名, 和当发现诸如非法分发图象的非法活动时, 就可以识别一个未经授权的分发, 而这正是一

个电子水印的最初目的。这是通过使用例如图 9 所示的系统 300 实现的。

系统 300 与图 8 所示系统 200 具有相同的结构，而由一个证书办公室 50 发出的匿名公共密钥则被提供给用户终端 20。

通常，为了证实一个签名信息，由被称之为证书办公室的一个组织颁发的证书被加到一个当检查所述签名信息时使用的公共密钥上。

所述证书办公室是这样一个组织，即它颁发用于指定给用户的公共密钥的证书以提供与所述公共密钥加密系统的请求相一致的公共密钥验证。即，证书办公室使用它自己的保密密钥提供与用户的公共密钥相关或与涉及所述用户的数据相关的签名，并为此目的准备和颁发一个证书。当一个用户从其他用户接收到具有所述证书的签名时，该用户使用证书办公室的公共密钥检查所述证书以验证由传送所述公共密钥的用户提供的证明（或至少是所述证书办公室已向所述用户提供了证明的事实）。VeriSign 和 CyberTrust 都是运行这种证书办公室的知名组织。

当在第二实施例嵌入处理的 1) 中一个代理检查一个签名以验证提供给一个用户的合同信息时，所述代理可以使用具有由所述证书办公室颁发的签名的公共密钥。

但是，由于公共密钥拥有者的姓名通常是写在所述证书中的，因此，在购买所述数据时不用提供用户的匿名。

另一方面，如果所述证书办公室保密相应的公共密钥和它们的拥有者，那么，一个拥有者的姓名就不能被写入所发出的用于一个公共密钥的证书中。用于被提供一个证书的公共密钥被称之为“具有证书的匿名公共密钥”。

在上述嵌入处理的 1) 中，当用户不仅向一个服务者传送了用于合同信息的签名之外还传送了一个具有证书的匿名公共密钥时，为了能够检查所述签名信息 S，所述用户可以在购买所述数字数据时保留所述匿名。因此，具有证书的所述匿名公共密钥将被传送各所述代理以用于用户验证。和当发现一个非法的事项和必须识别所述用户时，具有所述证书的公共密钥将被利用请求与对应于所述公共密钥拥有者姓名的用户姓名传送给所述证书办公室 50。

因此，当在第二实施例嵌入处理的 1) 和验证处理的 7) 被如下执行时，即当购买数字数据时的用户匿名可以被保持，但发现非法事项时，可以识别对犯罪事项负责的用户。

下面将详细描述如图 9 所示系统 300 执行的嵌入处理和验证处理。

在图8的系统200中使用的相同标号也被用于表示图9所示系统300的相应构件,并将省略对它们的详细描述。只对不同的部分进行详细描述。

由于除了在嵌入处理中的1)和验证处理中的1)以外所述处理与第二实施例的相应处理相同,所以,不再给出详细的解释。

[嵌入处理]

1')首先,在用户终端20中,合同发生器21提供用于请求所希望图象数据的合同信息以及与具有由证书办公室50颁发证书的匿名公共密钥对应的签名。与具有所述证书的匿名公共密钥一起,所述用户将合同信息传送给所述代理。

代理终端40使用具有所述证书的匿名公共密钥识别所接收的合同信息,并向服务者发出一个关于图象数据的请求。

然后,执行在第二实施例中的嵌入处理处理2)到9)。

在这种情况下,用户基本不会执行任何非法活动,所述代理也不会在原始图象数据中直接嵌入 $D1(U+D2(S))$ 。

当发现一个非法拷贝(非法图象)时,执行下面的验证处理。

[验证处理]

1)到6),首先,执行第二实施例验证处理的1)到6)。

7')当在1)提取到正确的用户信息 U' ($U' = U$)时,验证办公室30向证书办公室50提供用户信息 U' 和具有从所述合同信息中提取的证书的匿名公共密钥。验证办公室30请求证书办公室50识别其姓名与所述匿名公共密钥所有者姓名对应的用户。验证办公室30还请求所述服务者和所述代理提供所存储的散列值 $H2$ 和与由所述用户提供的散列值 $H2$ 相关的签名 A' ,并识别该签名 A' 。

然后,执行第二实施例验证处理中的8)到13)。

如上所述,根据第三实施例以及第二实施例,在发现一个非法活动之前不需要所述验证办公室30,并且,在发现一个非法活动之前不能执行任何非法活动。另外,只要上述验证处理是已知的,和所述服务者、所述代理和所述用户监视那个处理的结果,即使是没有所述验证办公室30的介入,也能够根据所述情况识别由它们之中任何一个进行的非法活动。

在第三实施例中,验证办公室30被附加提供给第二实施例中的系统200。但是,系统配置的修改没有被如此限制,证书办公室50可以被提供给第一实

实施例中的系统 100。在这种情况下，第一实施例嵌入处理中的处理 1) 对应于第三实施例的处理 1')，和第一实施例验证处理中的处理 8) 对应于第三实施例的处理 7)。

使用下面的图象格式可以存储第一到第三实施例中包括的各种数据和在与电子水印相关的嵌入处理期间获得的散列值。

根据下面一般的图象格式，例如，在各个步骤中传送的图象数据可以被存储在一个图象数据部分中，相应的散列值和它的签名可以被存储在一个图象标题部分中。另外，用户必须保留的一个散列值和它的伴随签名以及第二加密密钥可以被存储在一个图象标题部分中，而具有一个电子水印的图象数据可以被存储在所述图象数据部分中。

根据下面的 FlashPix™ 文件格式，包括所述散列值和所述签名的一般图象格式可以被作为数据存储每一层中。所述散列值和所述签名可以被作为属性信息存储在适当的位置处。

[关于一般图象格式的解释]

根据所述一般图象格式，一个图象文件被分成图象标题部分和图象数据部分，如图 10 所示。

通常，在图象标题部分中存储的是请求从一个图象文件中读出图象数据的信息，和用于解释一个图象内容的附加信息。在图 10 所示的例子中存储的是用于描述一个图象格式的名称、文件规模、图象的宽度和高度以及所述数据是否被压缩、分辨率、相对于图象数据存储位置的偏移、颜色调色板等的图象格式识别符。

这种图象格式的典型例子是微软的 BMP 格式和 CompuServe 的 GIF 格式。

[文件格式的解释]

根据下面的文件格式，存储图象标题部分中的属性信息和存储在图象数据部分中的图象数据被安置得更加接近地对应于一个结构并被存储在所述文件中。被结构的图象文件如图 11 和 12 所示。

所述文件中的各种特性和数据可以被作为存储区域和与 MS-DOS 的目录和文件对应的流进行访问。

在图 11 和 12 中，阴影部分是存储区域和非阴影部分是流。图象数据和图象属性信息被存储在所述流中。

在图 11 中，所述图象数据是根据它们不同的分辨率分级安置的，与每个

分辨率相关的一个图象被称之为一个子图象，并利用分辨率 0、1、...、或 n 表示。对于与每个分辨率相关的一个图象来讲，读出所述图象数据所需的信息被存储在子图象标题区域中，和所述图象数据被存储在子数据区域中。

通过由与其使用目的和内容相一致进行分类所规定的属性信息组成的特征集包括概要信息特征集、图象信息特征集、图象内容特征集和扩展列表特征集。

[关于每个特征集的解释]

概要信息特征集不是这个文件格式的固有部分，但对于一个文件的题目、姓名和作者以及略图图象的存储却是必须的。

一般的涉及一个存储单元（存储器）的信息被存储在 Com Obj. 流中。

图象内容特征集是一个用于描述图象数据存储方法的属性（见图 13）。关于这些属性，提供了图象数据层的数量、在其最大分辨率处图象的宽度和高度、在每个分辨率处图象的宽度、高度和颜色以及用于 JPEG 压缩的量化表或霍夫曼表的规定。

扩展列表特征集是一个用于在关于上述文件格式的基本规定中添加未包括信息的区域。

在 ICC 概貌区域中描述的是用于空间颜色转换的具体 ICC（国际颜色联合）转换概貌。

在图象信息特征集中存储的是各种能够被利用去使用图象数据的信息。例如，下面各种信息描述了一个图象是如何被取出的以及是如何被使用的：

- * 涉及一个取出方法的信息或用于数字数据的产生方法；
- * 涉及版权的信息；
- * 涉及一个图象内容的信息（一个图象中的人或景）；
- * 涉及一个用于照相的照相机的信息；
- * 涉及用于照相机（曝光、快门速度、焦距以及是否闪光等）的配置的信息；
- * 涉及数字照相机镶嵌式滤波器独有的分辨率的信息；
- * 涉及制片者姓名和所述影片名称和类型（负/正或彩色/黑白）的信息；
- * 当原作是一本书或其他印刷材料时涉及所述类型和尺寸的信息；和
- * 涉及被用于扫描一个图象的扫描器和软件应用的信息。

图 12 示出了一个图象文件，其中，被用于显示一个图象的视图参数和图

象数据被存储在一起。所述视图参数是一组当显示一个图象时用于调节旋转、放大/缩小、移位、颜色转换和滤波处理的系数。

在图 12 中，在全局信息特征集区域中写入例如是用于最大图象索引、用于最大修改项的索引、和涉及进行最后修改个人的信息的一个锁定属性表。

另外，源/结果闪烁象素图象目标构成了所述图象数据的实体，但同时需要源闪烁象素图象目标，而结果闪烁象素图象目标是可选的。一原始的图象数据被存储在所述源闪烁象素图象目标区域中，和提供使用所述观看参数进行图象处理所获得的图象数据被存储在结果闪烁象素图象目标区域中。

源/结果描述特征集是一个用于识别上述图象数据的特征集。图象 ID、禁止改变的特征集，和最后刷新数据和图象被存储在这个区域中。

在变换特征集区域中存储的是用于旋转、放大/缩小和移位一个图象、颜色转换矩阵、反差调节值的仿射转换系数和滤波系数。

[关于如何处理图象数据的解释]

与这个解释相关的是图象格式，该图象格式包括多个具有通过将一个图象分成多个铺砌所获得的不同分辨率的图象。

图 14 示出了由多个具有不同分辨率的图象构成的图象文件的例子。在图 14 中，具有最高分辨率的图象由 $X0$ 列 \times $Y0$ 行组成，和具有次高分辨率的图象由 $X0/2$ 列 \times $Y0/2$ 行组成。在所述列和行等于或小于 64 个象素之前或在所述列和行彼此相等之前，所述列的数量和行的数量基本上被减少 $1/2$ 。

作为图象分层的结果，在一个图象文件中需要一定数量的层，为一般图象格式所解释的图象属性信息和标题信息以及图象数据也被需要用于位于每层处的一个图象（见图 10）。在一个图象文件中层的数量、在它的最大分辨率处的一个图象的宽度和高度、具有各种分辨率的一个图象的宽度、高度和颜色以及压缩方法被存储在图象信息特征集区域中（见图 13）。

在每层处每个分辨率的图象被分成多个铺砌，其中的每个铺砌是 64×64 个象素，如图 15 所示。当一个图象被从左上部分开始分成 64×64 个象素的多个铺砌时，在右缘或下缘处的一个铺砌的一部分中可能发生空白区。在这种情况下，最右边的图象或最低的图象被重复插入以便构成一个 64×64 个象素的铺砌。

在这个 FlashPix™ 格式中，使用 JPEG 压缩或单一颜色或非压缩方法存储用于各个铺砌的图象数据。所述 JPEG 压缩是一种被 ISO/IEC JTC1/SC29 国际

标准化的图象压缩技术，有关解释将不在这里给出。单一颜色方法是一种当构成一个铺砌的所有象素具有相同的颜色时，所述铺砌被表示为单一的颜色，从而并不记录各种象素值。这种方法可以很容地用于使用计算机图象设备产生的图象。

被如此分成多个铺砌的图象数据被例如存储在图 11 所示的子图象数据流中，所述铺砌的总数、各个铺砌的尺寸、数据开始的位置和所述的数据压缩方法被存储在子图象标题区域中（见图 16）。

在第一到第三实施例中，可以使用各种方法嵌入所述电子水印信息。

另外，也可以使用诸如响应一个加密键的用于更换所述位配置的各种方法执行所述第一到第三加密。

另外，可以将散列值和它的签名提供给将被传送的所有数据。

在这些实施例中，在电子水印信息嵌入处理期间执行所述第一到第三加密，以避免第三实体获得存储在所述服务者、代理和用户处的信息。但是，可以执行 DES（数据解密标准）密码技术或散列函数以避免第三实体在通信路径上进行线路搭接或更换数据。

另外，在所述第一到第三实施例中，所述服务者（或作者）负责检测非法的数据分发。但是，只要提供了所述电子水印提取装置，即使是他或她不知道用于检测第一加密或第二加密的保密密钥，任何用户也都可以检测一个非法的数据分发和被非法分发的用户信息。当检测到非法数据分发发生时，用户只需要通知即将开始执行所述验证处理的服务者。因此，检测非法分发的处理并不局限于所述服务者。

在所述图象数据中不仅可以嵌入用户信息 U，而且可以嵌入诸如版权信息和涉及一个图象数据分发状态的信息的必要信息。另外，为了嵌入保密信息，所述服务者或代理只需要在第一加密之后执行嵌入处理，以便除了所述签名信息之外，在所述图象数据中嵌入由所述第一加密执行的信息。所述用户信息 U 不总是在第一加密之前被嵌入（在这种情况下，用户信息 U 的检测可以只由所述服务者、代理或知道用于所述第一加密的保密密钥的个人执行）。

当用户是一个共享一个打印机或一个终端的第二实体时，该用户的签名信息和所述第二加密密钥包括所述签名信息和用于所述公用打印机或终端的加密信息。

来自所述服务者（或作者）的第一被加密信息可以在一个网络上或使用

CD-ROM被广泛分发,即使是在没有由所述用户在合同信息基础上请求分发的情况下也是如此。

与所述用户相关的签名信息S不是必须由所述公共密钥加密方法产生,但是,可以由用户在合同信息的基础上规定的信息(例如,编码数)。

在美国,为了使用用于40位或更多位的加密,需要一个密钥管理办公室去管理一个加密密钥以避免未授权的密码技术使用。因此,验证办公室30也能够作为所述密钥管理办公室进行服务。当所述验证办公室30预先提供一个第二加密密钥的管理时,验证办公室30通过执行与非法图象相关的监视其本身就能够执行所述验证处理1)到3)。所述服务者的第一加密密钥可以通过相同的验证处理或通过其他的密钥管理办公室进行管理。所述服务者和所述用户的密钥可以由所述密钥管理办公室产生和分发。

另外,可以分级提供多个代理以代替单一的代理。在这种情况下,负责分级结构的特定代理可以执行所述处理,从而使所述负责的代理或所述多个代理可以执行所述协议以便规定将要负责的代理。

另外,在这些实施例中,在接收一个请求的基础上,所述服务者(或作者)可以响应向所述代理传送所述原始数据的第一被加密数据 $E1(G)$ 或 $E1(G+M)$ 。但是,所述服务者可以预先向所述代理传送数据 $E1(G)$ 或 $E1(G+M)$ 。

由所述代理执行的第三加密不影响最终获得的图象数据G。但是,所述图象数据G受经过处理的第三加密的影响,借此在第三加密之后嵌入所述用户信息U或借此在第三加密之后嵌入所述签名信息S。

当其上存储有软件程序码、用于执行在第一到第三实施例中所述主机和终端功能的步骤的一个存储媒体被提供给一个系统或服务者装置、代理或用户时,或当在所述系统或装置中的计算机(或CPU或MPU)可以通过读出存储在所述存储媒体上的所述程序码执行所述步骤时,本发明的上述目的可以被实现。

在这种情况下,从所述存储媒体读出的程序码可以被用于执行上述实施例的功能。上面存储有所述程序码的所述存储媒体构成本发明。

用于通过这种程序的存储媒体可以例如是ROM、软盘、硬盘、光盘、磁光盘、CD-ROM、CD-R、磁带或非易失存储卡。

另外,本发明的范围不仅包括当由所述计算机读出和执行所述程序码时可执行的第一到第三实施例的功能的情况,而且还包括根据包括在所述程序码中

的指令，当运行于所述计算机上的执行一部分或所有实际处理时执行上述实施例功能的情况。

再有，本发明包括下述情况，即从一个存储媒体读出的程序码被写入到安装在插入到所述计算机中的一个功能扩展板上的一个存储器中或安装到连接到一个计算机上的功能扩展单元上的一个存储器中，安装在所述功能扩展板或功能扩展单元上的CPU执行一部分或全部实际处理以便执行包括在所述第一到第三实施例中的功能。

如上所述，根据第一到第三实施例，可以通过第二实体（代理）嵌入涉及第三实体（用户）的信息。在这种情况下，第三实体不能执行一个非法活动。另外，由于这个信息受到只有第一实体（服务者或作者）知道的密码技术（由所述第一加密装置使用的第一加密和密码技术）或只有第三实体知道的一个密码技术（由所述第二加密装置使用的第二加密和密码技术）的影响，所以，第二实体不能被直接嵌入到涉及第三实体的原始数据信息（用户信息U或签名信息S）中。

因此，在一个分级网络中可以避免非法的数据分发，并提供一个安全系统。另外，能够很容易地实现所述的用户匿名。

（第四实施例）

下面结合图7讨论本发明的第四实施例。

例如利用图17所示的系统100执行本发明的电子水印方法。所述系统100应用了本发明的电子信息分发系统。

具体地说，系统100是一个由多方（未示出）构成的网络系统，包括在第一实体一侧处的终端10（此后称之为第一终端）、第二实体一侧处的终端20（此后称之为第二终端）和验证办公室一侧处的终端30（此后称之为验证终端）。各方在所述网络上交换数据。

所述第一终端10包括：合同识别单元11，用于从第二终端20接收数据；电子水印嵌入单元12，用于接收例如所述合同识别单元11的输出和图象数据（数字数据）；第一加密单元13，用于接收所述电子水印嵌入单元12的输出；和第一解密单元14，用于从所述第二终端20接收数据。用于第一加密单元13和第一解密单元14的数据被传送给所述第二终端20。

所述第二终端20包括：

合同发生器21，用于将数据传送给所述第一终端10的合同识别单元11；

签名发生器 22; 电子水印嵌入单元 23, 用于从所述签名发生器 22 和第一终端 10 的第一加密单元 13 接收数据; 第二加密单元 24, 用于从所述电子水印嵌入单元 23 接收数据; 和第二解密单元 25, 用于从第一终端 10 的第一解密单元 14 接收数据。来自第二解密单元 25 的数据被作为具有一个电子水印的图象数据输出。来自第二加密单元 24 的数据传送给第一终端 10 的第一解密单元 14 和验证终端 30。

所述验证终端 30 包括: 第二解密单元 31, 用于从第二终端 20 的第二加密单元 24 接收数据; 和电子水印嵌入单元 32, 用于接收来自第二解密单元 31 的数据。来自所述电子水印识别单元 32 的数据被传送给第一终端 10 和第二终端 20, 来自第二解密单元 31 的数据被传送给第一终端 10 的第一解密单元 14。

在根据这个实施例如此配置的电子信息分发系统中, 所述嵌入处理被分类到用于从服务者或作者向图 4 或图 5 所示的代理传送数字数据的第一嵌入处理和从所述代理向所述用户传送数字数据的第二嵌入处理。在这个实施例中, 随后的协议与第一和第二嵌入处理所使用的一个相同。作为整体, 首先执行所述第一嵌入处理, 然后执行所述第二嵌入处理。

在下面的解释中, 对于所述第一嵌入处理, 所述第一实体表示一个服务者或一个作者, 第二实体表示一个代理。对于所述第二嵌入处理, 所述第一实体表示所述代理, 而第二实体表示一个用户。因此, 至少是由所述代理使用的终端包括提供给图 17 所示第一终端 10 和第二终端 20 的所有处理器。

下面将结合图 17 描述用于执行第一和第二实施例的特定协议。根据这个协议, 只有第一实体可以获得诸如所述方法和保密密钥的涉及第一加密的信息, 而只有第二实体可以获得涉及第二加密的信息。但是, 应当注意, 对于这些加密处理来讲, 存在如下特性, 即首先执行考虑到这些特性的加密处理, 所以能够解密被加密的数据。此后, 所述加密处理由“Ei()”表示, 解密处理由“Di()”表示和涉及电子水印的嵌入处理由“+”表示。

下面描述由如此配置的系统 100 执行的处理。首先解释电子水印嵌入处理。

[嵌入处理]

1) 首先, 第二终端 20 的第二实体从第一终端 (第一实体) 请求具有其签名的所希望的图象数据。被请求的数据是一个签名信息, 该信息是由合同发生器 21 产生的, 此后称之为合同信息。

2) 在第一终端 10 的第一实体中, 合同识别单元 11 使用所述第二实体的签名以识别所接收的信息, 然后使用所述合同信息准备用户信息 U。电子水印嵌入单元 12 在所请求的图象数据 G 中嵌入由所述合同识别单元 11 准备的用户信息 U。第一加密单元 13 对其中已经被所述电子水印嵌入单元 12 嵌入所述用户信息 U 的图象数据 (G+U) 执行第一加密 $E1()$, 并将所获得的数据传送给第二终端 20。因此, 第二终端 20 接收第一被加密图象数据 $E1(G+U)$ 。

3) 在第二终端 20 中, 签名发生器 22 使用第二实体的保密密钥产生签名信息 S。电子水印嵌入单元 23 在由所述第一终端装置 10 传送 (分发) 的第一被加密图象数据 $E1(G+U)$ 中嵌入由所述签名发生器 22 产生的签名信息 S。第二加密单元 24 对已经由所述电子水印嵌入单元 23 嵌入签名信息 S 的第一被加密图象数据 $E1(G+U)+S$ 执行第二加密。然后将所获得的图象数据传送给验证终端 30。因此, 验证终端 30 接收第二被加密图象数据 $E2(E1(G+U)+S)$ 。

第二加密单元 24 产生一个用于所述第二被加密图象数据 $E2(E1(G+U)+S)$ 并将被其传送给验证终端 30 的散列值 H2。然后, 所述第二加密单元 24 提供一个用于所述散列值 H2 的签名, 并且, 除了所述签名信息 S 和所述第二加密密钥之外, 还将该签名传送给具有涉及所述电子水印的保密信息的验证终端 30。所述保密信息构成了一个涉及嵌入位置和检测一个电子水印所需的强度的信息, 且该信息被使用与所述验证终端 30 共享的其他加密方法加密。

所述散列值是一个通过计算随机函数 $h()$ 获得的一个值。所述随机函数是一个很少引起冲突的压缩函数。在这种情况下冲突将意味着对于不同的值 $x1$ 和 $x2$ 来讲, $h(x1) = h(x2)$ 。所述压缩函数是一个用于将一个具有规定位长的位串转换成具有不同位长的位串的函数。因此, 所述散列函数是一个函数 $h()$, 利用该函数 $h()$, 具有规定位长的一个位串被转换成具有不同位长的位串, 对于这个函数, 可以很容易地得到满足 $h(x1) = h(x2)$ 条件的值 $x1$ 和 $x2$ 。由于满足 $y = h(x)$ 的值 x 不容易从任意值 y 中得到, 因此, 所述散列函数是一个单向函数。与这种散列函数相关的特定例子是 MD (报文摘要) 5 和 SHA (安全散列算法)。

4) 验证终端 30 识别从所述第二终端 20 接收的具有所述散列值 H2 的签名, 并确认所述散列值 H2 与用于传送的所述散列值相匹配。在确认所述匹配之后, 第二解密单元 31 解密从第二终端 20 接收的第二被加密图象数据 $E2(E1(G+U)+S)$, 并从中提取所述签名信息。电子水印识别单元 32 检查所述签名

信息 S ，如果该签名信息是正确的，使用与所述验证终端 30 相关的签名准备所述验证信息。最后，验证终端 30 向第一终端 10 传送从第二终端 20 接收的第二被加密图象数据 $E2(E1(G+U)+S)$ 和散列值 $H2$ 以及它的附带签名以及用于它们的验证信息和它的签名。

5) 在第一终端 10 中，所述第一实体识别从所述验证终端 30 接收的验证信息和它的附带签名，和第二被加密图象数据 $E2(E1(G+U)+S)$ 以及散列值 $H2$ 和它的附带签名。在这个确认处理完成之后，第一解密单元 14 解密第二被加密图象数据 $E2(E1(G+U)+S)$ 的第一被加密部分以获得接下来将被传送给第二终端 20 的图象数据 $E2(G+U)+D1(E2(S))$ 。

6) 在第二终端 20 中，第二解密单元 25 解密从第一终端 10 接收的图象数据 $E2(G+U)+D1(E2(S))$ 的第二被加密部分，并提取其中已经嵌入一个电子水印的图象数据 G_e 。因此，包括所述电子水印的图象数据 G_e 被表示为 $G_e=G+U+D1(S)$ 。这意味着用于受所述第一解密影响的第二实体的用户信息 U 和签名信息 S 已经被作为电子水印嵌入到所述原始图象数据中。

如果在处理 4) 由于所述第一实体或第二实体进行了一个非法活动而使验证终端 30 没有验证所述电子水印信息，那么，有关该效果的一个通知将被传送给第一和第二终端 10 和 20。因此，当在此时终止一个买卖时，即使是所述第一实体不能够获得所述数据的价格，此时它也能够避免所述图象数据被第二实体非法获得；或即使是所述第二实体不能获得所述图象数据，此时它也不必向所述第一实体交付所述数据的价格。因此，由于既不是第一实体也不是第二实体获得利益或受到损失，所以，所述非法活动的进行变得毫无意义。

具体地说，当执行一个电子水印处理时，在第一加密处理中，构成所述第二实体的代理也能够获得包括一个通过在由构成所述第一实体的所述服务者或作者输出的原始数据中嵌入它自己的签名信息 S 而准备的电子水印的图象数据 G_e 。应当注意，当与所述第一嵌入处理相关的所述用户信息和签名信息是 $U1$ 和 $S1$ 时，所述代理获得的包括一个电子水印的图象数据 G_e 是 $G_e=G+U+D1(S1)$ 。

此后，以相同的方式（所述代理是第一实体）执行第二嵌入处理，而包括一个电子水印并由所述代理获得的图象数据 G_e 被用做所述原始数据。然后，用做第二实体的所述用户可以获得包括一个电子水印的图象数据 $G_e=G+U1+D1(S1)+U2+D3(S2)$ 。在第二嵌入处理中的用户信息和签名信息是 $U2$ 和 $S2$ ，和由所述代理执行的加密由 $E3()$ 表示，而所述解密被表示为 $D3()$ 。

当发现一个非法拷贝（非法图象）时，能够通过执行随后的简单验证处理很容易地识别进行了非法活动的一方。这个验证处理被分解成与第一嵌入处理对应并由所述服务者或作者和代理执行的第一验证处理和与第二嵌入处理对应并由所述代理和所述用户执行的第二验证处理。首先执行所述第一验证处理，然后执行所述第二验证处理。

在第一验证处理中，所述用户信息和签名信息是 $U1$ 和 $S1$ ，和由所述代理执行的加密和解密是 $E3()$ 和 $D3()$ 。在第二验证处理中，所述用户信息和签名信息是 $U2$ 和 $S2$ 。所述图象数据不受电子水印信息的删除和修改的影响。

[验证处理]

1) 在第一验证处理中，第一终端 10 的第一实体从被发现的非法图象数据 G' 中 $G' = G + U' + D1(S')$ 中提取 U' 。另外，第一实体执行与所述非法图象数据 G' 相关的第一加密并提取签名信息 S' 。当没有提取到所述用户信息 U' 时，它将确定所述第一实体进行了一个非法活动。

2) 当在所述第一验证处理中提取到了一个正确的签名信息 S' ($S' = S$) 时，启动所述第二验证处理。在该第二验证处理中执行相同的处理。当发现所述正确的签名信息时，它确定所述第二实体进行了一个非法活动。这是由于当所述第一实体不了解正确的签名信息时只有第二实体应当准备所述正确的签名信息。

3) 当没有能够提取到正确的签名信息 ($S' \neq S$) 时，它确定所述第一实体进行了一个非法活动。

根据第四实施例的电子水印方法，利用第一和第二终端 10 和 20 执行数字数据的加密和用于一个电子水印的嵌入处理，和利用验证终端 30 执行正确电子水印信息的加密和识别。因此，即使当第一实体和第二实体都各自准备了一个非法拷贝，也能够很容易地检测出所述非法活动，另外，也能够很容易地识别所述非法活动的犯罪者。

另外，根据这个方法，由于所述验证办公室检查第一嵌入处理和第二嵌入处理的结果，所以，不可能进行串通，因此，将不会发生服务者或作者和代理和用户的串通。即使是发生这种串通，也能够很容易地检查一个非法活动。在所述验证办公室是可信的前提下建立这个处理的安全保障。

(第五实施例)

近来，正在逐步使用在网络上传输货币，即被称之为电子货币的资金传输处理。由于正如一般的现金支付一样，不识别电子现金传输拥有者的姓名，所以必须附加一个匿名。如果这个匿名的附加是不可能的，产品的销售者就应当从涉及其产品的购买者和使用的电子传输信息中获得这个信息和不能保护用户的秘密。因此，保护用户的秘密和保护授权给使用一个电子水印的建造者的版权是同等重要的。

因此，在第五实施例，将一个用户的匿名提供给购买者，当发现诸如一个非法图象分发的非法活动时，就可以识别未经授权的分发，而这就是一个电子水印的目的。这是通过使用例如图 18 所示系统 200 实现的。

系统 200 具有与第四实施例系统 100 相同的结构，而由所述证书办公室 40 颁发的匿名公共密钥证书被提供给第二终端 20。

通常，为了鉴定所述签名信息，由被称之为证书办公室的一个组织颁发的证书被附加到当检查所述签名信息时使用的公共密钥上。

所述证书办公室是向一个指定用户颁发公共密钥证书以便提供与所述公共密钥加密系统的请求相一致的公共密钥鉴定的一个组织。即，所述证书办公室使用它自己的保密密钥提供与一个用户的公共密钥相关的签名，或与涉及所述用户数据相关的签名，并为此目的准备和发出一个证书。当一个用户从其他用户接收到伴有一个证书的签名时，所述用户使用所述证书办公室的公共密钥检查所述证书以验证由所述曾经传送所述公共密钥的用户提供的鉴定（或至少，所述证书办公室已经向所述用户提供了所述鉴定）。VeriSigh 和 CyberTrust 两者都是很著名地运行这种证书办公室的组织。

当在第四实施例的第二嵌入处理的处理 2) 处一个代理检查一个签名以验证发送给相关用户的合同信息时，所述代理可以使用具有由图 18 所示证书办公室 40 颁发的签名的公共密钥。但是，由于所述公共密钥拥有者的姓名通常是被写入所述证书中的，所以，在购买数据时不必提供用户匿名。

另一方面，如果证书办公室 40 保密相应的公共密钥和它的拥有者，那么，该用户的姓名就不能被写入为一个公共密钥所颁发的证书中。此后将用于用户公共密钥的匿名证书称之为“匿名公共密钥证书”，被提供这种证书的公共密钥被称之为“具有证书的匿名公共密钥”。在上述第二嵌入处理的处理 1) 处，当用户不仅向一个服务者发送合同信息，而且还发送与所述合同信息相关的签名信息以及伴有一个证书的匿名公共密钥从而使得可以检查所述签名信息 S

时,那么,当购买所述数字数据时,该用户可以保存匿名。

因此,伴有所述证书的匿名公共密钥被作为将被用于用户验证的信息传送给代理,当发现一个非法事项和必须识别用户时,必须利用与和所述公共密钥的拥有者姓名对应的用户姓名相关的请求将伴有所述证书的匿名公共密钥传送给所述证书办公室 40。因此,在第二嵌入处理的处理 1) 和 2) 以及存在第二实施例的第二验证处理的处理 1) 如下执行,即当购买所述数字数据时可以保留用户匿名,而当发现一个非法事项时,可以识别用户对所述事项犯罪的响应。

下面将详细描述由图 18 所示系统 200 执行的嵌入处理和验证处理。

[嵌入处理]

1) 首先,在第二终端 20,合同发生器 21 提供用于请求所希望图象数据的合同信息和与伴有证书办公室 40 所颁发的证书的一个匿名公共密钥对应的签名。与伴有所述证书的匿名公共密钥一起,第二终端 20 还要向第一终端 10 传送所述合同信息。

2) 在第一终端 10,合同识别单元 11 使用证书办公室 40 的公共密钥检查第二实体的公共密钥。所述合同识别单元 11 还使用第二实体的匿名公共密钥识别与所述合同信息相关的签名,并在完成所述确认处理之后,使用至少合同信息或所述匿名公共密钥准备用户信息。电子水印嵌入单元 12 在图象数据 G 中嵌入由所述合同识别单元 11 准备的用户信息 U。第一加密单元 13 对图象数据 G 执行第一加密 $E1()$,并将所获得的的数据传送给第二终端 20。由此,第二终端 20 接收第一被加密的图象数据 $E1(G+U)$ 。

由于处理 3) 到 6) 与第四实施例的这部分相同,所以这里不对它们再进行解释。

[验证处理]

1) 在第二验证处理中,第一终端 10 从所发现的非法图象数据 G_{in} 中提取用户信息。第一终端 10 还对非法图象数据 G_{in} 执行第一加密并从中提取签名信息。然后第一终端 10 向证书办公室 40 传送所提取的用户信息和从所述合同信息中获得的匿名公共密钥,并请求与所述匿名公共密钥对应的第二实体的姓名。当没有提取到所述用户信息时,它确认第一实体进行了一个非法活动。

处理 2) 和 3) 与第四实施例的该处理相同。

如上所述,根据第五实施例,当购买数字数据时,用户也可以保留与所述

验证办公室相关的他或她的匿名。

(第六实施例)

在第六实施例中,对图4或5所示的所述服务者或作者经过代理向用户分发数字的整个处理进行解释。下面将结合附图19解释本发明的第六实施例。具体地说,利用图19所示的系统300执行根据本发明第六实施例的电子水印方法,所述系统300应用了本发明的电子信息分发系统。

在第六实施例中,系统300是一个由包括在服务者一侧上的终端50(此后称之为服务者终端)、代理一侧上的终端60(此后称之为代理终端)用户一侧上的终端70(此后称之为用户终端)和在验证办公室一侧上的终端30(此后称之为验证终端)的多个实体(未示出)构成的网络系统。各实体在所述网络上交换数字数据。

服务者终端50包括:第一加密单元51,用于接收例如图象数据(数字数据);第一解密单元52,用于接收来自用户终端70和验证终端30的数据。来自第一加密单元51的数据被传送给所述代理终端60,来自第一解密单元52的数据被传送给一个终端70。

代理终端60包括:合同识别单元61,用于接收来自用户终端70的数据;电子水印嵌入单元62,用于接收用户终端50的第一加密单元51的输出。从电子水印单元61输出的数据被传送给用户终端70和验证终端30。

用户终端70包括:合同发生器71,用于向代理终端60的合同识别单元61传送数据;签名发生器72;电子水印嵌入单元73,用于从签名发生器72和代理终端60的电子水印嵌入单元62接收数据;第二加密单元74,用于接收来自电子水印嵌入单元73的数据;和第二解密单元75,用于从服务者终端50的第一解密单元52接收数据。来自第二解密单元75的数据被作为包括一个电子水印的图象数据传送。来自第二加密单元74的数据被传送给服务者终端50的第一解密单元52和验证终端30。

验证终端30包括:第二解密单元31,用于从代理终端60的电子水印单元62和用户终端70的第二加密单元74接收数据;和电子水印识别单元32,用于从第二解密单元32接收数据。电子水印单元32的数据被提供给服务者终端50的第一解密单元52。

下面解释由如此构成的系统300执行的处理。对于图19所示的协议,只有所述服务者或作者可以得到涉及诸如所述方法和它的保密密钥的第一加密

的信息,而只有所述用户可以得到涉及所述第二加密的信息。但是,应当注意,对于这些加密处理来讲,存在某些特性,考虑到这些特性,首先执行加密处理,然后可以解密这些被加密的数据。当在下面的解释中使用图5所示的分级系统时,通过利用所述服务者替换所述作者,可以将这个解释应用于图4所示的系统。

[嵌入处理]

1) 首先,用户终端70请求代理终端60提供它所希望的伴有它的签名的图象数据。被请求的数据是由所述合同发生器71产生且此后被称之为合同信息的信息(用户的签名信息)。在代理终端60处,合同识别单元61使用所述的用户签名信息识别所接收的合同信息,然后将一个请求图象数据的请求传送给服务者终端(作者)50。在接收这个请求的基础上,服务者终端50的第一加密单元51执行图象数据G的第一加密 $E1()$ 并将所获得的数据传送给代理终端60。

2) 在代理终端60中,合同识别单元61使用从用户终端70接收的合同信息准备用户信息U。电子水印嵌入单元62在由所述服务者终端50传送的第一被加密图象数据 $E1(G)$ 中嵌入由所述合同识别单元61产生的用户信息U。因此,用户终端70接收包括用户信息U的第一被加密图象数据 $E1(G)+U$ 。

代理终端60的电子水印嵌入单元62向验证终端30传送涉及一个电子水印的保密信息。所述保密信息是一个涉及与检测电子水印相关的嵌入位置和强度并利用与所述验证终端30共享的另外一种加密方法加密的信息。

3) 在用户终端70中,签名发生器22使用用户的保密密钥产生签名信息S。电子水印嵌入单元73在已经由代理终端60传送(分发)的第一被加密图象数据 $E1(G)+U$ 中嵌入由所述签名发生器72产生的签名信息S。第二加密单元74对已经由所述电子水印嵌入单元73嵌入了签名信息S的第一被加密图象数据 $E1(G)+U+S$ 执行第二加密,并将所产生的的数据传送给验证终端30。因此,验证终端30接收第二被加密的图象数据 $E2(E1(G)+U+S)$ 。

与此同时,用户终端70的第二加密单元74产生与将被传送给验证终端30的第二被加密的图象数据 $E2(E1(G)+U+S)$ 相关的散列值H2。然后,第二加密单元74提供一个与所述散列值H2相关的签名,并与涉及电子水印和第二加密密钥的保密信息一起传送给验证终端30。

4) 所述验证终端30识别从用户终端70接收的伴有散列值H2的签名,并

确认所述散列值 $H2$ 与用于传送所述数据的散列值相匹配。在完成了这个确认处理之后,第二解密单元 31 解密从用户终端 70 接收的第二被加密的图象数据 $E2(E1(G)+U+S)$, 并从中提取用户信息 U 和签名信息 S 。然后,电子水印识别单元 32 检查用户信息 U 和签名信息 S , 如果所述信息 U 和 S 是正确的,使用验证终端 30 的签名准备验证信息。最后,验证终端 30 向服务者终端 50 传送从用户终端 70 接收的第二被加密的图象数据 $E2(E1(G)+U+S)$ 、散列值 $H2$ 和它的签名信息以及用于它们的验证信息和它的签名。

5) 在服务者终端 50 中,作者识别从验证终端 30 接收的验证信息和它的签名和所述第二被加密的图象数据 $E2(E1(G)+U+S)$ 、散列值 $H2$ 和它的签名。在这个确认处理完成之后,第一解密单元 52 解密第二被加密的图象数据 $E2(E1(G)+U+S)$ 的第一被加密部分,以获得图象数据 $E2(G)+D1(E2(U+S))$, 然后这个数据被传送给用户终端 70。

6) 在用户终端 70 中,第二解密单元 75 解密从服务者终端 50 接收的图象数据 $E2(G)+D1(E2(U+S))$ 的第二被加密部分并提取其中已经嵌入一个电子水印的图象数据 G_e 。因此,所述图象数据 G_e 和所包括的电子水印由 $G_e=G+D1(U+S)$ 表示。这意味着受所述第一加密影响的用户信息 U 和签名信息 S 已经被作为电子水印嵌入到了原始图象数据中。

如果在处理 4) 验证终端 30 没有验证所述电子水印是正确的,由于所述作者或用户进行了一个非法活动,关于这个事实的一个通知被传送给服务者终端 50、代理终端 60 和用户终端 70。由于即使是在这个时候终止所述交易也不会使任何一方得到利益或受到损失,所以,非法活动的进行无关紧要。当发现一个非法拷贝(非法图象) G_e' 时,可以通过执行下面的简单验证处理很容易地识别进行了非法活动的一方。应当注意,所述图象数据是受电子水印信息的修改和删除的影响的。

[验证处理]

1) 首先,在服务者终端 50 中,作者执行所述非法图象数据 G_e' 的第一加密并提取用户信息 U 。当没有提取到所述用户信息 U 时,它确定所述作者进行了一个非法活动。

2) 当提取到了一个正确的用户信息 U 时,从对所述非法图象数据 G_e' 进行第一加密获得的数据中提取签名信息。

3) 当提取到了一个正确的签名信息时,它确定用户进行了一个非法的活

动。这是由于当所述代理可能不了解所述签名信息时，只有所述用户和作者能够准备正确的签名信息。

4) 如果没有提取到所述的正确的签名信息，它确定所述作者进行了一个非法活动。

根据第六实施例的电子水印方法，数字数据的加密和电子水印的嵌入处理是由服务者终端 50、代理终端 60 和用户终端 70 执行的，正确的电子水印信息的加密和识别是由验证终端 30 执行的。因此，当作者、代理或用户分别准备了一个非法拷贝时，可以很容易地检测所述非法活动和能够很容易地识别所述非法活动。另外，根据这个方法，由于验证办公室检查第一加密处理和第二加密处理的结果，所以，不可能执行串通，因此，所述服务者或作者与代理和用户的串通是不可能发生的。即使是这种串通可能发生，也可以很容易地检测该非法活动。这个处理的安全性是以所述验证办公室是可信赖的为基础的。

(第七实施例)

在第七以及第六实施例中，将对图 4 或图 5 所示服务者或作者经过代理向用户分发数字数据的整个处理进行解释。本发明的第七实施例将结合图 20 予以描述。具体地说，根据第七实施例的电子水印方法是由图 20 所示的系统 400 执行的，所述系统 400 应用了本发明的电子信息分发系统。

在第七实施例中，系统 400 是一个由包括服务者终端 50、代理终端 60、用户终端 70 和验证终端 30 的多个实体（未示出）构成的网络系统。各个实体在所述网络上交换数据。

服务者终端 50 包括：第一加密单元 51，用于接收例如图象数据（数字数据）；第一解密单元 52，用于从用户终端 70 和验证终端 30 接收数据。来自第一加密单元 51 的数据被传送给代理终端 60，而来自第一解密单元 52 的数据被传送给用户终端 70。

代理终端 60 包括：合同识别单元 61，用于从用户终端 70 接收数据；电子水印嵌入单元 62，用于接收合同识别单元 61 和用户终端 50 的第一加密单元 51 的输出；和电子水印嵌入单元 63，用于从用户终端 70 接收数据。从电子水印单元 61 输出的数据被传送给用户终端 70 和验证终端 30。另外，电子水印嵌入单元 63 的输出被传送给服务者终端 50 和验证终端 30。

用户终端 70 包括：合同发生器 71，用于向代理终端 60 的合同识别单元 61 传送数据；第二加密单元 74，用于从代理终端 60 的电子水印嵌入单元 62

接收数据, 和第二解密单元 75, 用于从服务者终端 50 的第一解密单元 52 接收数据。来自第二解密单元 75 的数据被作为包括一个电子水印的图象数据传送。来自第二解密单元 74 的数据被传送给代理终端 60 的电子水印嵌入单元 63。

验证终端 30 包括: 第二解密单元 31, 用于从代理终端 60 的电子水印嵌入单元 63 和用户终端 70 的第二加密单元 74 接收数据; 电子水印识别单元 32, 用于从所述第二解密单元 31 和从代理终端 60 的电子水印嵌入单元 63 接收数据。所述电子水印单元 32 的数据被提供给服务者终端 50 的第一解密单元 52。

下面解释由如此构成的系统 400 所执行的处理。对于图 20 所示的协议, 诸如所述方法和它的保密密钥的涉及第一加密的信息只有所述服务者或所述作者可以得到, 而涉及第二加密的信息只有所述用户可以得到。但是, 应当说明, 对于这些加密处理来讲, 存在某些特性, 首先执行考虑到这些特性的加密处理, 然后可以对被加密的数据解密。当在下面的解释中使用图 5 所示的分级系统时, 通过利用所述服务者替换所述作者, 可以将这个解释应用于图 4 所示的系统。

[嵌入处理]

1) 首先, 用户终端 70 请求代理终端 60 提供它所希望的具有它的签名的图象数据。被请求的信息是由所述合同发生器 71 产生并在此后称之为合同信息的信息(用户的签名信息)。在代理终端 60 中, 合同识别单元 61 使用所述用户的签名识别所接收的合同信息, 然后, 将该请求传送给与所述图象数据相关的服务者终端(作者) 50。在接收该请求的基础上, 服务者终端 50 的第一加密单元 51 执行图象数据 G 的第一加密 $E1()$ 并将获得的数据 $E1(G)$ 传送给代理终端 60。

2) 在代理终端 60 中, 合同识别单元 61 使用从用户终端 70 接收的合同信息准备用户信息 U。电子水印嵌入单元 62 在由所述服务者终端 50 传送的第一被加密图象数据 $E1(G)$ 中嵌入由所述合同识别单元 61 产生的用户信息 U。因此, 用户终端 70 接收包括用户签名信息 U 的第一被加密图象数据 $E1(G) + U$ 。

3) 在用户终端 70 中, 第二加密单元 74 执行从代理终端 60 接收的第一被加密图象数据 $E1(G) + U$ 的第二加密, 并将所获得的图象数据 $E2(E1(G) + U)$ 传送给代理终端 60。签名发生器 72 产生只有用户才能够准备的签名信息, 和与第二被加密图象数据 $E2(E1(G) + U)$ 一起将该签名信息传送给代理终端 60。另外, 第二加密单元 74 将第二加密保密密钥传送给验证终端 30。

4) 在代理终端 60 中, 电子水印嵌入单元 63 在第二被加密图象数据 $E2(E1(G)+U)$ 中, 即在这两种情况下从用户终端 70 接收的信息中嵌入签名信息 S , 并将所获得的数据传送给验证终端 30。由此, 验证终端 30 接收第二被加密的图象数据 $E2(E1(G)+U+S)$ 和它的签名信息。

在此同时, 代理终端 30 产生用于将被传送给验证终端 30 的第二被加密图象数据 $E2(E1(G)+U+S)$ 的散列值 $H2$ 。然后, 代理终端 30 提供用于所述散列值 $H2$ 的签名, 并与涉及电子水印和第二加密保密密钥的保密信息一起将它传送给验证终端 30。所述保密信息是涉及到检测电子水印所需的嵌入位置和强度并利用与验证终端 30 共享的其他加密方法加密的信息。

5) 验证终端 30 识别从代理终端 60 接收的伴有所述散列值 $H2$ 的签名, 并确认所述散列值 $H2$ 与用于传送数据的散列值相匹配。在确认处理完成之后, 电子水印嵌入单元 32 在从代理终端 60 接收的第二被加密的图象数据 $E2(E1(G)+U+S)$ 中提取签名信息 S 。第二解密单元 31 解密从用户终端 70 接收的第二被加密图象数据 $E2(E1(G)+U+S)$, 并从中提取用户信息 U 。

电子水印嵌入单元 32 检查用户信息 U 和签名信息 S 。如果用户信息 U 和签名信息 S 是正确的, 使用验证终端 30 的签名准备验证信息。最后, 验证终端 3 向服务器终端 50 传送从所述代理终端 60 接收的第二被加密图象数据 $E2(E1(G)+U)+S$ 、散列值 $H2$ 和它的伴随签名以及用于它们的验证信息和它的签名。

6) 在服务器终端 50 中, 作者识别从所述验证终端 30 接收的验证信息和它的伴随签名, 以及第二被加密图象数据 $E2(E1(G)+U)+S$ 、散列值 $H2$ 以及它的伴随签名。在这个确认处理完成之后, 第一解密单元 52 解密第二被加密图象数据 $E2(E1(G)+U)+S$ 的第一被加密部分以获得接下来将被传送给用户终端 70 的图象数据 $E2(G)+D1(E2(U)+S)$ 。

7) 在用户终端 70 中, 第二解密单元 75 解密从服务器终端 50 接收的图象数据 $E2(G)+D1(E2(U)+S)$ 的第二被加密部分, 并提取其中已经被嵌入一个电子水印的图象数据 G 。因此, 包括所述电子水印的图象数据 G 由 $G=G+D1(U+D2(S))$ 表示。这意味着受所述第一解密影响的用户信息 U 和受第一和第二解密影响的用户的签名信息被作为一个电子水印嵌入到了所述原始图象数据中。

如果在处理 5) 中, 验证终端 30 没有验证所述电子水印信息, 那么, 由

于作者或用户中的一个进行了分非法活动，所以，关于这个事实的一个通知将被传送给所述服务者终端 50、代理终端 60 和用户终端 70。由于即使是在这个时候终止所述交易，它们中的任何一方都不会获得利益或受到损失，所以，非法活动的进行无关紧要。当发现一个非法拷贝（非法图象）G' 时，可以通过随后的简单验证处理识别进行了非法活动的一方。应当说明所述图象数据不受电子水印信息修改和删除的影响。

[验证处理]

1) 首先，在服务者终端 50 中，作者对所述非法图象数据 G' 执行第一加密和提取所述用户信息 U。当没有提取到所述用户信息 U 时，它确定所述作者进行了一个非法活动。

2) 当提取到一个正确的用户信息 U' 时，服务者终端 50 向验证终端 30 提供第一被加密图象数据 G' 和用户信息 U'，并请求对它们进行检查。验证终端 30 对第一被加密图象数据 G' 执行第二加密（它的加密功能没有示出），并提取签名信息。

3) 当提取到一个正确的签名信息时，它确定所述用户进行了一个非法活动。

4) 当没有提取到一个正确的签名信息时，它确定所述作者进行了一个非法活动。

根据第七实施例的电子水印方法，数字数据的加密处理和与电子水印相关的嵌入处理是由服务者终端 50、代理终端 60 和用户终端 70 执行的，正确电子水印信息的加密和识别是由验证终端 30 执行的。因此，即使当作者、代理或用户都分别准备了一个非法拷贝，也很容易检测所述非法活动。另外，也能够很容易地识别进行非法活动的一方。另外，根据这个方法，由于验证办公室检查第一嵌入处理和第二嵌入处理的结果，所以，不能执行所述串通。因此，服务者或作者与代理和用户的串通将不会发生。即使是这种串通发生了，也能够很容易检测这种串通。这个处理的安全性是以所述验证办公室是可信赖的为基础的。

(第八实施例)

根据第八实施例，在用于图 18 所示第六实施例的配置中，当用户购买数字数据时，与和在第五实施例中一样，所述用户可以保留该用户的匿名，而当发现一个诸如分发非法图象的非法活动时，可以使用例如图 21 所示的系统 500

识别进行了非法活动的一方。除了用户终端 70 从证书办公室 40 接收匿名公共密钥证书之外，系统 500 与第六实施例中的系统 300 配置相同。

在这个实施例以及第五实施例中，如果证书办公室 40 保密相应的公共密钥和它们拥有者的姓名，那么，拥有者的姓名就不能被输入到为一个公共密钥颁发的证书中。在第六实施例嵌入处理的处理 1) 中，当用户不仅向服务者传送合同信息，而且还传送与该合同信息相关的签名和将被用于检查签名信息 S 并伴有证书的匿名公共密钥，那么，当购买数字数据时，所述用户就能够保留所述匿名。

因此，伴有所述证书的匿名公共密钥被传送给所述用户作为与该用户相关的识别信息。然后，当发现一个非法活动时，伴有所述证书的匿名公共密钥被传送给证书办公室 40 和请求与所述公共密钥对应的用户姓名以便能够识别所述用户。因此，当在第六实施例的嵌入处理中的处理 1) 和验证处理中的处理 1) 被如下改变时，即当购买数字数据时能够保留用户的匿名，而当发现一个非法活动时能够识别进行了非法活动的一方。

应当说明，当购买数字数据时，用户可以保留所述匿名，而当发现一个非法活动时，通过如下改变第七实施例所述嵌入处理的处理 1) 和验证处理中的处理 1) 能够识别进行了非法活动的一方。

下面将详细描述由图 21 所示系统 500 执行的嵌入处理和验证处理。

[嵌入处理]

1) 首先，在用户终端 70 中，合同发生器 71 提供一个用于请求所希望数据以及与所述伴有由所述证书办公室 40 颁发的匿名公共密钥对应的签名的合同信息。然后合同发生器 71 向代理终端 60 传送所述匿名公共密钥和伴有所述签名的合同信息。在代理终端 60 中，合同识别单元 61 使用所述匿名公共密钥识别所接收的合同信息，并请求来自所述作者的图象数据。在接收该请求的基础上，服务者终端 50 中的第一加密单元 51 执行图象数据 G 的第一加密 E1 ()，并将所获得的图象数据 E1 (G) 传送给代理终端 60。

由于处理 2) 到 6) 与第六实施例的相应部分相同，这里不再进行描述。

[验证处理]

1) 在服务者终端 50 中，第一加密单元 51 执行所发现的非法图象数据 G' 的第一加密，并从中提取用户信息。服务者终端 50 向证书办公室 40 传送所提取到的用户信息和使用所述合同信息识别的匿名公共密钥，并请求与所述匿名

公共密钥对应的用户姓名。当没有提取到所述用户信息时，它确定所述作者进行了一个非法活动。

处理2)到4)与第六实施例的该处理相同。

如上所述，根据第八实施例，当购买数字数据时，用户可以保留涉及验证办公室的的匿名。

包括在第四实施例到第八实施例的图象数据和在用于电子水印信息的嵌入处理期间获得的散列值的各种数据都可以使用上述图象格式存储。例如，根据一般的图象格式，在各个步骤传送的图象数据可以被存储在一个图象数据部分中，相应的散列值和它的签名可以被存储在图象标题部分中。另外，用户必须保留的散列值以及它的伴随签名和第二加密密钥可以存储在图象标题部分中，而具有电子水印的图象数据可以存储在图象数据部分中。

在第四到第八实施例中，可以使用各种方法嵌入所述电子水印信息。

另外，可以使用诸如用于与加密密钥相一致地改变位配置的各种方法执行所述第一和第二加密。另外，所述散列值和它的签名可以被用于需要传送的所有数据。在这些实施例中，在电子水印信息嵌入处理期间执行第一加密和第二加密以避免服务者、用户和代理获得彼此所存储的信息。但是，可以使用 DES（数据加密标准）密码技术或散列函数以避免第三实体在通信路径上窃取和更换数据。

另外，在第四到第八实施例中，所述第一实体（服务者或作者）负责非法数据分发的检测。但是，只要提供了所述电子水印提取装置，即使是任何一个用户不知道用于第一加密或第二加密的保密密钥，他或她也都可以检测已经被非法分发的非法数据分发和用户信息。当检测到发生了一个非法数据分发时，所述用户只需要通知与已经开始验证处理相关的第一实体。因此，检测非法分发的处理不局限于第一实体。

第一实体或代理不仅可以在图象数据中嵌入用户信息U，还可以嵌入诸如版权信息和涉及图象数据分发状态的信息的其他所需信息。另外，为了嵌入保密信息，所述第一实体只需要在第一加密之后执行嵌入处理，从而除了签名信息以外，还可以在所述图象数据中嵌入受第一加密影响的信息。用户信息U并不总是在第一加密之前被嵌入，它可以在所述第一加密之后嵌入（在这种情况下，用户信息U的检测可以只通过第一实体或知道用于第一加密的保密密钥的个人执行）。

当所述第二实体是共享一个打印机或一个终端的用户时,用于第二实体的签名信息和第二加密可以包括用于被公用的打印机或终端的签名信息和加密系统。即使是在没有合同信息的基础上由第二实体请求的它的分发,来自第一实体的第一被加密信息也可以被广泛地在一个网络上或使用 CD-ROM 进行分发。用于第二实体的签名信息 S 不必须通过所述公共密钥加密方法产生,也可以是在合同信息基础上由所述用户规定的信息(例如,代码号)。

在美国,为了使用用于 40 位或更多位的加密,需要一个密钥管理办公室管理加密密钥以避免版权的未经授权使用。因此,验证办公室 30 也能够作为密钥管理办公室进行服务。当所述验证办公室提供一个第二加密密钥的先期管理时,验证办公室本身可以通过执行对非法图象的监视执行验证处理的 1) 到 3)。第一实体的第一加密密钥可以由同一个验证办公室或其他的密钥管理办公室管理。第一实体和第二实体的密钥可以由密钥管理办公室产生和分发。

另外,代替单一的代理,可以分级提供多个代理。在这这种情况下,负责分级结构的一个特定代理可以执行所述代理执行的处理,或各个代理可以执行所述协议以规定将要负责的一个代理。当如图 5 所示只提供了一个代理时,可以省略涉及所述代理的用户信息 U 的嵌入。

再有,在接收一个请求的基础上,所述作者做出响应将原始数据 G 的第一被加密数据 E1(G) 传送给所述代理。但是,该作者可以预先向所述代理传送所述数据 E1(G)。

在第六和随后描述实施例中的代理不能执行加密 E3() 和解密 D3()。但是,可以在首先从所述作者接收数据之后使用所述加密处理 E3() 加密所述数据,或在数据被传送给所述作者之前使用解密处理 D3() 解密所述数据。

如上所述,根据上述电子水印嵌入方法和系统,利用多个装置或实体分发或处理数据加密处理和电子水印嵌入处理。所发生的由所述装置或实体执行的至少是一个加密处理和电子水印嵌入处理的合法性是由除了上述装置或实体之外的一个装置或实体验证的。因此,当数据被在一个分级网络上非法拷贝和分发时,可以精确地识别所述非法活动和进行了所述非法活动的一方。结果是,可以避免非法活动的进行,并可以提供防止数据非法分发的安全系统。另外,这个系统可以很容易地被应用到用于保存用户匿名和防止数据非法拷贝的密钥管理办公室。

下面结合附图 22 到 26 描述本发明的第九到第十二实施例。

图 22 简要示出了在它的一方内根据本发明第九实施例一个电子信息分发系统的配置。作为它的内容, 服务者 S 保持电子信息, 代理 A1 到 Am 与所述服务者 S 制定一个用于分发电子信息的合同。通过发出多个请求, 代理 A1 到 Am 从服务者 S 获得它们所希望的数据作为电子水印, 并存储所接受的数据。

用户 U11 到 Uln 与所述代理 A1 制定一个合同用于获得电子信息服务。用户向代理 A1 传送多个请求, 以请求它所存储内容的分发, 并在接受它们的基础上, 将它们作为电子水印进行存储。代理 A2 到 Am 和用户 U21 到 2n 和 Uml 到 Umn 之间的关系与在代理 A1 和用户 U11 到 Uln 之间的存在的关系相同。

在这个实施例中, 下述的电子水印叠加方法被应用于图 22 所示的系统。下面结合图 23 到 26 描述用于所述电子水印叠加方法的特定实施例。

所述处理被分成处理 1 和处理 2, 在处理 1 中, 图 22 中的服务者 S 将作为电子信息的图象数据传送给代理 A1 到 Am, 在处理 2 中, 代理 A1 到 Am 将图象数据传送给用户 U11 到 Ymn。在下面使用所述电子水印叠加方法的实施例中, 相同或基本相同的协议被用于处理 1 和 2。首先执行处理 1, 然后执行处理 2。下面将解释用于处理 1 和 2 的特殊协议。

(第九实施例)

下面结合图 23 描述第九实施例。

所述网络系统包括第一实体, 即终端 10、第二实体, 即终端 20 和验证办公室终端 30。所述第一实体, 即终端 10 包括: 合同识别单元 11, 用于从终端 20 接收数据; 第一电子水印嵌入单元 12, 用于接收例如图象数据(数字数据); 第一加密单元 13, 用于接收所述第一电子水印嵌入单元 12 的输出; 第一解密单元 14, 用于从终端 20 接收数据; 第二电子水印嵌入单元 15, 用于从终端 20 和第一解密单元 14 接收数据; 和散列发生器 16, 用于接收所述第二电子水印嵌入单元 15 的输出。所述第一加密单元 13 和散列发生器 16 的输出被传送给终端 20。第二电子水印嵌入单元 15 的输出被传送给散列发生器 16 和终端 20。

第二实体终端 20 包括: 合同发生器 21, 用于向终端 10 的合同识别单元 11 传送数据; 签名发生器; 第二加密单元 24, 用于从终端 10 的第一加密单元 13 接收数据; 第二解密单元 25, 用于从终端 10 中的第二电子水印嵌入单元 15 和第一加密单元 14 接收数据; 散列识别单元 27, 用于从终端 10 的第二电子水印嵌入单元 15 和散列发生器 16 接收数据。由第二解密单元 25 产生的数据被作为伴有一个电子水印的数据输出。由第二加密单元 25 产生的数据被传送给

终端 10 的第一解密单元 14. 由签名发生器 22 产生的数据被传送给终端 10 的第二电子水印单元 15.

在上述系统中, 涉及诸如所使用方法和保密密钥的第一加密处理的信息仅仅是所述服务者可以得到的信息; 涉及第二加密处理的信息仅仅是第二实体可以得到的信息. 但是, 应当说明, 这些加密处理的特性考虑到了首先执行所述加密处理, 使用所述解密处理可以解密一个消息.

此后, 所述加密处理被表示为 " $E1()$ ", 解密处理被表示为 " $D1()$ " 和涉及电子水印的嵌入处理被表示为 "+".

下面解释由图 23 所示系统执行的处理. 首先解释电子水印嵌入处理.

[嵌入处理]

1) 首先, 第二实体, 即终端 20 从终端 10 请求伴有用户签名的所希望图象数据. 所请求的数据是由合同发生器 21 产生并在此后称之为合同信息的信息 (用于第二实体的签名信息).

2) 在终端 10 中, 合同识别单元 11 使用用于所述第二实体的签名信息识别所接收的合同信息, 并在此之后, 使用所述合同信息准备用户信息 U . 第一电子水印嵌入单元 12 在所请求的图象数据 G 中嵌入由所述合同识别单元 11 准备的用户信息 U . 第一加密单元 13 对已经由第一电子水印嵌入单元 12 嵌入了用户信息 U 的图象数据 $(G+U)$ 执行第一加密处理 $E1()$, 并将所生成的图象数据传送给终端 20. 由此, 终端 20 接收第一被加密的图象数据 $E1(G+U)$.

3) 在终端 20 中, 第二加密单元 24 对从终端 10 接收的第一被加密的图象数据 $E1(G+U)$ 执行第二加密处理, 并将所生成的第二被加密的图象数据 $E2(E1(G+U))$ 传送给终端 10.

在此同时, 在第二实体中, 签名发生器 22 使用它自己的保密密钥产生签名信息 S 并将该信息传送给终端 10.

4) 在终端 10 中, 第一解密单元 14 解密从终端 20 接收的第二被加密图象数据 $E2(E1(G+U))$ 的第一被加密部分. 第二电子水印嵌入单元 15 识别从终端 20 接收的签名信息 S . 第二电子水印嵌入单元 15 在由所述第一解密单元 14 产生的图象数据 $E2(G+U)$ 中嵌入所述签名信息 S , 并将所获得的图象数据传送给终端 20. 另外, 散列发生器 16 产生用于传送数据 $E2(G+U)+S$ 的散列值 $H1$, 为它签名, 和所获得的散列值 $H1$ 与图象数据 $E2(G+U)+S$ 一起被传送给终端 20. 结果是, 终端 20 接收图象数据 $E2(G+U)+S$ 和具有它的伴随签名的

散列值H1。

所述散列值是通过计算一个散列函数 $h()$ 获得的值, 所述随机函数是一个很少引起冲突的压缩函数。在这种情况下冲突意味着对于不同的值 x_1 和 x_2 来讲, $h(x_1) = h(x_2)$ 。所述压缩函数是一个用于将具有规定位长的位串转换成具有不同位长的位串。因此, 所述散列函数 $h()$ 是一个被用于将具有规定位长的一个位串转换成具有不同长度的位串的函数, 对于这个函数来讲, 满足 $h(x_1) = h(x_2)$ 的 x_1 和 x_2 是不容易发现的。由于不能从任意值 y 中很容易地获得满足 $y = h(x)$ 的值 x , 所以, 所述随机函数是一个单向函数。有关所述随机函数的特定例子是 MD (消息摘要) 或 SHA (保密散列算法)。

5) 终端 20 的散列识别单元 27 识别从终端 10 接收的散列值 H1 和它的伴随签名, 并确认散列值 H1 与使用数据 $E2(G+U)+S$ 产生的散列值相匹配。在完成所述确认处理之后, 存储数据 $E2(G+U)+S$ 和散列值 H1 以及它的伴随签名。

第二解密单元 25 解密数据 $E2(G+U)+S$ 的第二被加密部分, 并提取其中已经嵌入了一个电子水印的图象数据 G_u 。这指出在所述原始数据中已经嵌入了作为电子水印信息的用户信息 U 和第二被加密的签名信息 S。

如上所述, 根据这个实施例的电子水印嵌入方法, 由于所述第一实体完全负责电子水印信息的嵌入, 所以, 第二实体基本上不能够进行非法活动。所述第一实体直接从所述第二实体接收签名信息 S 并将它作为电子水印信息嵌入。但是, 由于经过嵌入处理的处理 5), 终端 20 获得的签名信息受只有该第二实体能够执行的第二加密的影响, 所以, 所述第一实体不能够通过直接在所述原始图象数据中嵌入签名信息 $D2(S)$ 控告第二实体犯罪。

当执行上述嵌入处理时, 在处理 1 中, 所述代理可以获得具有其中在所述服务者或作者的原始图象 G 中嵌入他或她的签名信息的一个电子水印的图象数据 G_u 。假设在处理 1 中用户信息和签名信息是 U_1 和 S_1 和在所述代理执行的加密和解密处理被表示为 $Ea()$ 和 $Da2()$, 具有由所述代理获得的所述电子水印的图象被表示为 $G_u = G + U_1 + Da2(S_1)$ 。当在处理 2 中在所述代理的图象数据 G_u 被作为原始数据使用的同时执行相同的嵌入处理时, 用户可以获得具有一个电子水印的图象数据 $G_{uu} = G + U_1 + Da2(S_1) + U_2 + Du2(S_2)$ 。在这种情况下, 假设在处理 2 中的用户信息和签名信息是 U_2 和 S_2 和由所述用户执行的加密和解密是 $Eu2()$ 和 $Du2()$ 。

当发现一个非法拷贝 G_w' 时, 通过随后的验证处理识别执行了所述非法活动的一方。这个验证处理被分成验证 1 和验证 2, 验证 1 对应于用于验证所述服务者、代理或作者和代理的处理 1, 验证 2 用于验证所述代理和用户。首先执行验证 1, 然后执行验证 2。在验证 1 中, 用户信息和签名信息被规定为 $U1$ 和 $S1$, 和由所述代理执行的加密和解密是 $Ea2()$ 和 $Da2()$ 。在验证 2 中, 用户信息和签名信息被规定为 $U2$ 和 $S2$, 和由用户执行的加密和解密是 $Eu2()$ 和 $Du2()$ 。

应当说明, 所述图象数据不受电子水印信息修改或删除的影响。

[验证处理]

1) 首先, 在与服务者 S 和代理 A 相关的验证 1 中, 在服务者一侧 (第一实体) 上的终端 10 从非法图象数据 $G_w' = G + U' + U2' + Da(S1') + Du2(S2')$ 中提取用户信息 $U1'$ 。当不能提取所述用户信息 U' 时, 它确定所述服务者 S 进行了一个非法活动。

2) 作为第一实体的服务者向所述验证办公室传送所述非法图象 G_w' 和所提取的用户信息 $U1'$, 并请求所述验证办公室 30 检查作为第二实体的代理 A 。

3) 验证办公室 30 请求第二实体传送存储在它之中的第二加密密钥。验证办公室 30 对所述非法图象 G_w' 执行第二加密以提取签名信息 $S1'$ 。

4) 如果提取到了正确的签名信息 $S1'$, 即 $S1' = S1$, 它确定作为第一实体的服务者没有进行所述非法活动, 程序控制向验证 2 运行。

5) 当在处理 4) 没有提取到正确的签名信息时, 即当 $S1' \neq S1$ 时, 验证办公室 30 检查数据 $Ea2(G + U1) + S1$ 和散列值 $H1$ 以及它的伴随签名 $S1$, 所有这些信息都是由作为第一实体的服务者 S 传送给作为第二实体的代理 A 的。验证办公室 30 确认所述散列值 $H1$ 与从 $Ea2(G + U1) + S1$ 获得的散列值相匹配。然后, 验证办公室 30 使用在处理 3) 由所述代理 A 传送的第二加密密钥解密数据 $Ea2(G + U1) S1$, 并提取其中已经被嵌入一个电子水印的图象数据 G_w 。

6) 当不能提取到其中已经被嵌入一个电子水印的正确图象数据时, 它确定代理 A 进行了一个非法活动。这意味着在处理 3) 中所述第二加密密钥是不正确的。

7) 当能够提取到其中已经被嵌入了一个电子水印的正确图象数据时, 它确定服务者 S 进行了一个非法活动。

下面解释当在处理 4) 确定所述服务者没有进行所述非法活动时所执行的

有关验证 2 的处理。在验证 2 中，从所述非法图象数据 $G_{u'}$ ($=G+U1'+U2'+Da2(S1')+Du2(S2')$) 中提取用户信息 U' 。当没有提取到所述用户信息 $U2'$ 时，它确定作为第一实体的代理 A 进行了所述非法活动。

在处理 2) 中，在验证 2 中用做第一实体的上述代理向验证办公室 30 传送所述非法图象数据和所提取到的用户信息 $U2'$ 并请求验证办公室 30 检查作为第二实体的所述用户 U。在处理 3)，验证办公室 30 请求所述第二实体传送存储在它之中的第二加密密钥，并通过对所述非法图象数据 $G_{u'}$ 执行第二加密提取签名信息 $S2'$ 。当提取到了正确的签名信息 S' 时，即当 $S2'=S2$ 时，它确定作为第二实体的用户进行了所述非法活动。

当没有提取到正确的签名信息 $S2'$ 时，即当签名信息 $S2'$ 与 $S2$ 不匹配时，在处理 5) 验证办公室 30 检查数据 $Eu2(G+U2)+S2$ 、散列值 $H1$ 和它的伴随签名 $S2$ ，所有的这些信息都是从作为第一实体的代理 A 传送给作为第二实体的用户 U 的。然后，验证办公室 30 确认散列值 $H1$ 与从数据 $Eu2(G+U2)+S2$ 获得的散列值相匹配，此后，验证办公室 30 使用由所述用户 U 传送的第二加密密钥解密数据 $Eu2(G+U2)+S2$ ，并提取其中已经被嵌入一个电子水印的图象数据 $G_{u'}$ 。

当没有提取到其中已经被嵌入一个电子水印的正确的图象数据时，它在处理 6) 确定作为第二实体的所述用户 U 进行了所述非法活动。这意味着由所述用户传送的第二加密密钥是不正确的。当能够提取到其中已经被嵌入一个电子水印的正确的图象数据时，在处理 7)，它确定作为第一实体的所述代理 A 进行了所述非法活动。

如上所述，对于验证 1 和验证 2 执行基本相同的处理，只需要改变关于第一实体和第二实体的定义。另外，可以以相同的方式识别进行了非法活动的一方。

从所述验证处理可以明显看出，验证办公室 30 的终端包括与终端 20 的第二加密单元 24、第二解密单元 25 和散列识别单元 27 相同的功能。

在上述实施例中，由于处理 1 和 2 是分开执行的，所以，串通是没有意义的。例如，即使是所述代理与所述用户串通，该用户也不能影响处理 1。另外，即使是所述服务者与所代理串通，或者是服务者与用户串通，所述用户和代理也都不能获得包括受由所述用户或所述代理执行的加密影响的一个电子水印的最终图象数据。

在发现一个非法图象之前并不需要验证办公室 30, 并且, 在发现一个非法图象之前不能确定已经执行了非法活动。另外, 只要上述验证处理是已知的, 和所述第一和第二实体监视所述处理结果, 那么, 即使是不包括所述验证办公室, 也能够根据所述状态检测由它们执行的非法活动。

(第十实施例)

最近, 已经使用了在网络上进行货币传送, 即被称之为电子现金的资金传送处理。由于一般的现金交付不需要识别电子现金传送拥有者的姓名, 因此, 需要获得一个匿名。如果不可能获得所述匿名, 产品的销售者应当从涉及购买者和其产品使用的电子现金传送信息中获得, 用户的秘密将不能得到保护。因此, 对用户秘密的保护和对授权于使用电子水印的一个创建者的版权的保护是同等重要的。

因此, 在第十实施例中, 用户的匿名将被提供给购买者, 并且当发现诸如图象非法分发的非法活动时, 它可以识别未经授权的分发者, 这是电子水印的最初目的。这是通过使用例如图 24 所示的系统实现的。

所述系统与第九实施例的系统 100 具有相同的结构, 而由证书办公室 40 颁发的匿名公共密钥证书被提供给用户终端 20。

通常, 为了鉴定签名信息, 由一个被称之为证书办公室的组织颁发的证书被加到当检查所述签名信息时使用的一个公共密钥上。

所述证书办公室是一个为指定给用户的公共密钥颁发证书以提供与所述公共密钥加密系统的请求相一致的公共密钥鉴定的组织。即, 证书办公室使用它自己的保密密钥为用户的公共密钥、或为涉及所述用户的数据提供签名, 和为这个目的准备和颁发证书。当用户从其他用户接收伴有一个证书的签名时, 该用户使用所述证书办公室的公共密钥检查所述证书以验证由传送所述公共密钥的用户提供的鉴定(或至少所述鉴定已经被证书办公室提供给了所述用户)。VeriSign 和 CyberTrust 是著名的运行这种证书办公室的组织。

当在第九实施例的嵌入处理中的处理 2) 处第一实体检查一个签名以确认传送给一个用户(第二实体)的合同信息时, 所述第一实体可以使用具有由图 24 中的证书办公室 40 颁发的一个签名的公共密钥。但是, 由于所述公共密钥拥有者的姓名通常被写入所述证书中, 所以, 在购买数据时不提供用户匿名。

另一方面, 如果证书办公室 40 保密相应的公共密钥和它的拥有者, 那么, 在颁发给一个公共密钥的证书中可以不写入拥有者的姓名。用于一个公共密钥

的匿名证书此后被称之为“匿名公共密钥证书”，和被提供这样一种证书的公共密钥被称之为“具有证书的匿名公共密钥”。在上述嵌入处理的处理1)中，当用户U向一个服务者不仅提供合同信息，而且还提供用于所述合同信息的签名以及伴有一个证书的匿名公共密钥从而使能签名信息S的检查时，那么，当购买数字数据时，该用户可以保留匿名。

因此，伴有所述证书的匿名公共密钥被作为将被用于验证用户U的信息传送给代理A。当发现一个非法事项和必须识别用户时，伴有所述证书的匿名公共密钥被利用一个和与所述公共密钥拥有者姓名对应的用户姓名相关的请求传送给证书办公室40。因此，当在第九实施例的嵌入处理中的处理1)和2)和验证处理中的处理1)和2)被如下执行时，购买数字数据时的用户匿名可以保留，但当发现非法事项时，能够识别对犯罪负责的用户。

下面详细描述由图24所示系统执行的嵌入处理和验证处理。

在图24所示的系统中，与图23所示系统中使用的相同标号被用于表示相应的构件，和只给出不同部分的解释。由于除了嵌入处理中的处理1)和2)和验证处理中的处理1)和2)以外，所述处理与第九实施例相同，所以，对于它们将不做详细解释。

[嵌入处理]

1) 首先，在第二实体(用户)终端20中，合同发生器21提供作为用于请求所希望图象数据、与伴有由证书办公室40颁发的一个证书的匿名公共密钥对应的签名的合同信息。第二终端20将所述的合同信息与匿名公共密钥和伴随证书一起传送给第一实体(代理)终端10。

2) 在第一实体终端10中，合同识别单元11使用所述证书办公室40的公共密钥检查属于第二实体(用户)的公共密钥。合同识别单元11使用第二实体的匿名公共密钥识别用于所述合同信息的签名，并在完成确认处理之后，使用至少是合同信息或匿名公共密钥准备的用户信息U。第一电子水印嵌入单元12在图象数据G中嵌入由所述合同识别单元11准备的用户信息U。第一加密单元13对图象数据G执行第一加密 $E1()$ ，并将所获得的数据传送给第二实体终端20。由此，第二实体终端20接收第一被加密的图象数据 $E1(G+U)$ 。

然后执行第九实施例中的处理3)到5)。

第十实施例嵌入处理中的处理1)和2)将被应用于前述的处理1)和2)。当对于一个代理来讲一般的匿名不是太重要时，保留用户匿名的秘密是非常重要的。

要的, 由所述于嵌入处理是在当所述代理将它的内容作为电子水印分发给所述用户时使用的, 所以在这个实施例中它是特别重要的。

因此, 作为对所述实施例的修改, 当图 23 所示第九实施例所示的系统被用于由服务者向代理分发电子信息时, 和当图 24 所示第十实施例所示系统被用于由所述代理向所述用户分发电子信息时, 分级系统将更加有效。即, 在所述分级系统中, 在保持向证书办公室 40 传送尽可能最小数量请求的同时, 能够保护所述用户的秘密。

[验证处理]

当将所述验证处理应用于第九实施例的验证处理 2 时, 它是非常有效的。因此, 下面的解释是在假设下述的处理 1) 和 2) 被应用于由所述代理和用户执行的验证, 即验证 2 的前提下给出的。此时, 假设在验证 1) 的处理 4 确定所述服务者 S 确实没有进行非法活动。

1) 首先, 在用于代理 A 和用户 S 的验证 2 中, 代理一侧 (第一实体) 的终端 10 从非法图象数据 $G_{\text{非法}}' = G + U1' + U2' + Da2(S1') + Du(S2')$ 中提取用户信息 $U2'$ 。当不能够提取用户信息 $U2'$ 时, 它确定代理 A 进行了一个非法活动。当能够提取所述用户信息 $U2$ 时, 所提取的用户信息 $U2$ 和从合同信息中获得的匿名公共密钥被传送给证书办公室 40 以请求与所述公共密钥对应的用户姓名。

2) 作为第一实体的代理 A 向验证办公室传送所述非法数据 $G_{\text{非法}}'$ 和所提取的用户信息 $U2'$, 并请求验证办公室检查其姓名与所述公共密钥对应的用户。

执行在第九实施例所述验证处理中的上述处理 3) 到 7)。

如上所述, 根据第十实施例, 当购买数字数据时, 所述用户可以相对于所述验证办公室保留匿名。

(第十一实施例)

下面结合图 25 描述第十一实施例。第十一实施例与第十实施例的不同之处在于不是使用第一实体终端 10, 而是使用第二实体终端 20 嵌入作为一个电子水印并与该第二实体相关的签名信息。与图 23 所用相同的标号也被用于图 25 所示的相应构件。下面将给出与第九实施例相同处理的解释。

终端 10 包括: 合同识别单元 11, 用于从终端 20 接收数据; 电子水印嵌入单元 12, 用于接收例如图象数据 (数字数据); 第一加密单元 13, 用于接收所述电子水印嵌入单元 12 的输出; 第一解密单元 14, 用于从终端 20 接收数

据; 散列识别单元 35, 用于从终端 20 和第一解密单元 34 接收数据; 和散列发生器 36, 用于接收第一解密单元 34 的输出。第一加密单元 13 和散列发生器 36 的输出被传送给终端 20。第一解密单元 34 的输出被传送给散列发生器 36 和终端 20。

第二实体终端 20 包括: 合同发生器 21, 用于向终端 10 的合同识别单元 11 传送数据; 签名发生器 22; 电子水印嵌入单元 43, 用于从签名发生器 22 和终端 10 的第一加密单元 13 接收数据; 第二加密单元 44, 用于从电子水印嵌入单元 43 接收数据; 散列发生器 46, 用于接收第二加密单元 44 的输出; 第二解密单元 45, 用于从终端 10 的第一解密单元 34 接收数据; 散列识别单元 47, 用于从终端 10 的第一解密单元 34 和散列发生器 36 接收数据。由第二解密单元 45 产生的数据被作为其中已经嵌入一个电子水印的数据输出。

由第二解密单元 44 产生的数据被传送给终端 10 的第一解密单元 34 和散列识别单元 35。由散列发生器 36 产生的数据被传送给终端 10 的散列识别单元 35。

下面将解释由图 25 所示系统执行的电子水印嵌入处理。

[嵌入处理]

由于处理 1) 和 2) 与第九实施例的该部分相同, 这里不再进行解释。

3) 在终端 20 中, 签名发生器 22 使用属于第二实体的保密密钥产生签名信息 S。

电子水印嵌入单元 43 在已经由终端 10 传送(分发)的第一被加密图象数据 $E1(G+U)$ 中嵌入由所述签名发生器 22 产生的签名信息 S。

第二加密单元 44 对其中已经由电子水印嵌入单元 43 嵌入了签名信息 S 的第一被加密图象数据 $E1(G+U)+S$ 执行第二加密。所获得的图象数据被传送给第一实体终端 10。

因此, 终端 10 接收第二被加密图象数据 $E2(E1(G+U)+S)$ 。

散列发生器 46 产生用于将被传送给终端 10 的第二被加密图象数据 $E2(E1(G+U)+S)$ 的散列值 $H2$ 。然后, 散列发生器 46 将一个签名提供给散列值 $H2$, 并利用除所述签名信息 S 以外涉及所述电子水印的一个保密信息将它传送给终端 10。

所述保密信息是涉及检测被与终端 10 共享的另一种加密方法加密的一个电子水印所需的嵌入位置和强度的信息。

4) 在终端 10 中, 散列识别单元 35 识别用于从用户终端 20 接收的散列值 H2 的签名, 确认所述散列值 H2 与将被传送数据的散列值相匹配。在完成所述验证处理之后, 存储所述的散列值 H2。

第一解密单元 34 解密从终端 20 接收的第二被加密图象数据 $E2(E1(G+U)+S)$ 的第一被加密部分, 并将所获得的图象数据传送给终端 20。

利用这种方式, 用户终端 20 接收图象数据 $E2(G+U)+D1(E2(S))$ 。

散列发生器 36 产生用于将被传送给终端 20 的图象数据 $E2(G+U)+D1(E2(S))$ 的散列值 H1。散列发生器 36 然后向所述散列值 H1 提供一个签名, 并将它传送给终端 20。

5) 在终端 20 中, 散列识别单元 47 识别从服务器终端 10 接收并用于散列值 H1 的签名, 并确认所述散列值 H1 与将被传送数据的散列值相匹配。在完成该确认处理之后, 存储所述散列值 H1。

第二解密单元 45 解密从终端 10 接收的图象数据 $E2(G+U)+D1(E2(S))$ 的第二被加密部分, 并提取其中已经被嵌入一个电子水印的图象数据 G_e 。

因此, 其中已经被嵌入一个电子水印的图象数据 G_e 被表示为 $G_e = G+U+D1(S)$ 。这意味着在原始图象数据 G 中嵌入了受第一解密影响的电子水印(用户信息)U 和电子水印(签名信息)。

存储其中已经被嵌入所述电子水印的图象数据 G_e 。

如上所述, 用户信息 U 不受加密的影响, 而签名信息 S 受第一解密的影响。

当执行上述嵌入处理时, 在处理 1 中, 所述代理可以获得其中已经嵌入一个电子水印的图象数据 G_e , 其中他或她的签名信息被嵌入到所述服务器或作者的原始图象 G 中。假设在处理 1 中的用户信息和签名信息是 U1 和 S1, 由用户执行的加密和解密是 $E_{s1}()$ 和 $D_{s1}()$, 由代理执行的加密和解密用 $E_a()$ 和 $D_{a2}()$ 表示, 由所述代理获得的其中已经被嵌入一个电子水印的图象用 $G_e = G+U1+D_{s1}(S1)$ 表示。当在代理的图象数据 G_e 被用做原始图象数据的同时在处理 2 中执行相同的嵌入处理时, 用户可以获得具有一个电子水印的图象数据 $G_e = G+U1+D_{s1}(S1)+U2+D_{a1}(S2)$, 其中, 由代理执行的加密和解密是 $E_{a1}()$ 和 $D_{a1}()$ 。在这种情况下, 假设在处理 2 中的用户信息和签名信息是 U2 和 S2。

当发现一个非法拷贝 G_e' 时, 如在第九实施例所述, 验证处理被分成验证 1 和验证 2, 所述验证 1 与用于验证服务器或作者和代理的处理 1 相对应,

而验证 2 用于验证所述代理和用户。首先执行验证 1, 然后执行验证 2。在验证 1 中, 用户信息和签名信息分别是 U 和 S , 由所述服务者执行的加密和解密分别表示为 $E_{s1}()$ 和 $D_{s1}()$ 。在验证 2 中, 用户信息和签名信息分别被规定为 U_2 和 S_2 , 由多数代理执行的加密和解密分别是 $E_{a1}()$ 和 $D_a()$ 。

应当说明, 如在第九和第十实施例一样, 所述图象数据不受电子水印信息修改和删除的影响。

[验证处理]

1) 首先, 在用于服务者 S 和代理 A 的验证 1 中, 在服务者一侧上的终端 10 (第一实体) 从非法图象数据 $G_{..}' = G + U' + U_2' + D_{s1}(S') + D_{a1}(S_2')$ 中提取用户信息 U_1' 。另外, 终端 20 对图象数据 $G_{..}'$ 执行第一加密和提取签名信息 S_1' , 当不能够提取到所述用户信息 U_1' 时, 它确定服务者 S 进行了一个非法活动。

2) 当提取到了一个正确的签名信息 S_1' 时, 即当 $S_1' = S_1$ 时, 服务者 S 向验证办公室 30 传送所述签名信息 S_1' , 即, 它确定作为第一实体的所述服务者没有进行所述非法活动。程序控制前进到验证 2。

3) 当在处理 2) 没有能够提取到所述正确的签名信息, 即 S_1' 与 S_1 不匹配时, 为了请求验证, 作为第一实体的服务者 S 向验证办公室 30 传送所存储的用于第二被加密图象数据 $E_{a2}(E_{s1}(G + U_1) + S_1)$ 的散列值以及它的伴随签名、第一加密密钥和涉及所述非法图象数据 $G_{..}'$ 的保密信息。

4) 在接收在处理 3) 的所述请求的基础上, 验证办公室 30 确定不能从所述非法图象数据 $G_{..}'$ 中提取正确的签名信息 S_1 。然后, 验证办公室 30 检查所传送的散列值 H_2 和它的伴随签名以便确认第二被加密图象数据 $E_{a2}(E_{s1}(G + U_1) + S_1)$ 的散列值与已经传送的散列值 H_2 相匹配。

在完成所述确认处理之后, 验证办公室 30 解密第二被加密图象数据 $E_{a2}(E_{s1}(G + U_1) + S_1)$ 的第一被加密部分并获得图象数据 $E_{a2}(G + U_1) + D_{s1}(E_{a2}(S_1))$ 。验证办公室 30 确认用于所获得数据的散列值与由作为第二实体的所述代理 A 保存的散列值 H_1 相匹配。此时, 还识别用于散列值 H_1 的签名。

5) 当在处理 4) 用于数据 $E_{a2}(G + U_1) + D_{s1}(E_{a2}(S_1))$ 的散列值与散列值 H_1 不匹配时, 它确定作为第一实体的服务者 S 进行了一个非法活动。这意味着在嵌入处理的处理 4) 和在验证处理中的处理 4) 中用于第一加密的保密密钥是不同的。

6) 当两个散列值匹配时, 验证办公室请求作为第二实体的代理 A 解密在验证处理的处理 4) 中获得的数据 $Ea2(G+U1)+Ds1(Ea2(S1))$ 的第二被加密部分。验证办公室 30 检查来自所生成图象数据的签名信息 $S1$ 。

7) 当不能提取到正确的签名信息 $S1$ 时, 即当 $S1'$ 与 $S1$ 不匹配时, 它确定所述代理 A 进行了一个非法活动。

8) 当提取到了一个正确的签名信息时, 它确定不是所述代理, 而是所述服务者 S 进行了一个非法活动。

下面解释当它确定所述服务者 S 没有进行一个非法活动时所执行的验证处理 2。在验证 2 中, 作为处理 1), 从非法图象数据 $G_{..}' = G+U1' +U2' +Ds1(S1') +Da1(S2')$ 中提取用户信息 $U2'$ 。另外, 对图象数据 $G_{..}'$ 执行第一加密 $Ea1()$ 以提取签名信息 $S2'$ 。当不能提取用户信息 $U2'$ 时, 它确定代理 A 进行了一个非法活动。

当如上述处理 2) 提取到正确的签名信息 $S2'$ 时, 即当 $S2' = S2$ 时, 所述代理 A 向验证办公室 30 传送签名信息 $S2'$ 以确定所述用户 U 是否进行了一个非法活动。

这是由于所述签名信息 $S2'$ 仅仅是由不知道所述签名信息 $S2'$ 的所述用户 U、所述服务者 S 和所述代理 A 准备的。应当说明, 所述签名信息的合法性是通过确定由所述合同信息预先规定的预定信息是否能够通过使用与当产生所述签名信息时用户使用的保密密钥对应的公共密钥输出进行验证的。

当不能提取所述合同信息 $S2$ 时, 当在处理 3) 时, 为了请求验证, 作为第一实体的代理 A 向验证办公室 30 传送用于所存储第二被加密图象数据 $Eu2(Ea1(G+U1+U2+Ds1(S1))+S2)$ 和它的伴随签名、用于第一加密的保密密钥和涉及所述非法图象 $G_{..}'$ 的保密信息。

在处理 4), 验证办公室 30 确定从所述非法图象 $G_{..}'$ 中不能提取到正确的签名信息 $S2$ 。验证办公室 30 检查散列值 $H2$ 和所传送的散列值, 并确认用于第二被加密图象数据 $Eu2(Ea1(G+U1+U2+Ds1(S1))+S2)$ 的散列值和已经传送的散列值 $H2$ 相匹配。在完成所述确认处理之后, 验证办公室 30 解密第二被加密图象数据 $Eu2(Ea1(G+U1+U2+Ds1(S1))+S2)$ 的第一被加密部分和获得数据 $Eu2(G+U1+U2+Ds1(S1))+Da1(Eu2(S2))$ 。另外, 验证办公室 30 确认用于所获得图象的散列值和已经由作为第二实体的用户 U 所存储的散列值 $H1$ 相匹配。

当用于数据 $Eu2(G+U1+U2+Ds1(S)) + Da1(Eu2(S2))$ 的散列值与散列值 $H1$ 不匹配时, 如在上述处理 5), 它确定作为第一实体的代理 A 进行了一个非法活动。当所述两个散列值相匹配时, 验证办公室 30 请求作为第二实体的用户解密数据 $Eu2(G+U1+U2+Ds(S1)) + Da1(Eu2(S2))$ 的第二被加密部分。从所述被解密的数据中提取签名信息 $S2$ 。

当不能提取到正确的签名信息 $S2$ 时, 它确定作为第二实体的用户进行了一个非法活动。但是, 当提取到了一个正确的签名信息 $S2$ 时, 它确定作为第一实体的所述代理进行了一个非法活动。

如上所述, 验证 1 和验证 2 是根据相同的处理陆续执行的, 只有第一和第二实体的定义需要改变。另外, 可以以相同的方式识别进行了非法活动的一方。

就单独执行验证 1 和验证 2, 在发现一个非法活动之前不需要所述验证办公室, 并且在发现一个非法活动之前, 不能进行非法活和不需要提供所述验证办公室等方面来将, 第十一实施例与第九实施例相同。

(第十二实施例)

图 26 示出了本发明的第十二实施例。图 24 和 25 中相同的标号被用于表示执行相同处理的构件, 对它们的解释将予以省略。根据第十二实施例, 利用第十一实施例的配置, 为了使用户的私密能够得到保护, 如在第十实施例一样, 用户 S 将合同信息与伴随有由所述证书办公室 4 颁发证书的一个公共密钥一起传送给代理 A。

关于在这个实施例中的嵌入处理, 利用第十实施例中的处理 1) 和 2) 替换第十一实施例中的处理 1) 和 2), 随后的处理与第十一实施例的处理相同。当这个嵌入处理被应用于由所述代理向用户分发电子信息时, 它与第十实施例的嵌入处理一样有效。

当这个实施例的验证处理被应用于第十一实施例的验证处理 2 时是有差别的, 下面将描述这些差别。首先, 在用于代理 A 和用户 U 的验证 2 中, 代理一侧上的终端 10 (第一实体) 从已经发现的非法图象数据 $G_{..}' = G+U1' + U2' + Da1(S1') + Du(S2')$ 中提取用户信息 $U2'$ 。

代理 A 向证书办公室 40 传送用户信息 $U2'$ 和从合同信息中获得的匿名公共密钥, 并请求与所述公共密钥对应的用户姓名。当不能提取到用户信息 $U2'$ 时, 它确定所述代理 A 进行了一个非法活动。再有, 对非法图象数据 $G_{..}' = G+U1'$

+U2' +Da1 (S1') +Du (S2') 执行第一加密, 提取签名信息 S2' 。由于所述连续的处理与第十一实施例的验证 2 相同, 所以, 不再进行解释。

当不能提取签名信息 S2' 时, 它确定所述服务者进行了一个非法活动。当提取到了所述用户信息 U2' 时, 所述代理 A 向证书办公室 40 传送所述用户信息 U2' 和从所述合同信息中获得的匿名公共密钥, 并请求与所述公共密钥对应的用户姓名。然后, 作为第一实体的代理 A 向验证办公室传送所述非法图象数据 G_u'、提取用户信息 U2' 和请求检查与所述公共密钥对应的用户姓名。

在上述的实施例中, 可以使用各种方法嵌入电子水印信息, 诸如在例如 1996 年 9 月 11 日在第 53 届 Information Processing Institute National Assembly(信息处理学会全国大会)由 Shimizu, Numao, Morimoto(IBM, Japan)发表的“使用象素块的静态图形数据的隐匿”、或在 NEC 研究工业技术报告 95-10 中由 I. J. Cox, J. Kilian, T. Leighton 和 T. Shamoon(NEC)等人发表的“用于多媒体的保密扩频水印”中描述的已知方法。

另外, 第一加密和第二加密所使用的方法也可以使用诸如用于与一个加密密钥相一致地改变位配置的加密方法的各种方法实现。

另外, 在嵌入处理的 2) 中, 所述散列值和签名不包括在将被传送给用户终端 20 的图象数据 E1 (G+U) 中。但是, 一个散列值和它的签名可以被提供给所述数据以确定通信路径是否已经被修改。

另外, 在所述电子水印信息嵌入处理中执行第一加密和第二加密, 以避免所述服务者和用户被通知由其他方所存储的信息。但是, DES(数据加密标准)加密和散列函数可以被用于避免第三实体在通信路径上窃听和修改数据。

再有, 在各实施例中, 第一实体负责检测非法数据的分发。但是, 只要提供电子水印提取装置, 即使是他或她都不知道用于第一加密和第二加密的保密密钥, 任何一个用户也都可以检测数据和用户信息的非法分发。当检测到数据的非法分发时, 用户仅仅需要通知与将被开始进行验证处理相关的服务者。因此, 非法分发的检测并不局限于所述第一实体。

第一实体的终端 10 在所述图象数据中不仅可以嵌入用户信息 U, 而且在需要时可以嵌入诸如版权信息和涉及一个图象数据分发状态的其他信息。另外, 为了嵌入保密信息, 服务者终端 10 仅仅需要在第一加密之后执行所述嵌

入处理,以便,除了签名信息之外,还能够在所述图象数据中嵌入受所述第一加密影响的信息。所述用户信息U不总是在第一加密之前被嵌入,可以在第一加密之后被嵌入(在这种情况下,用户信息U的检测可以只有服务者,或由已经知道用于所述第一加密的保密密钥的个人执行)。

当第二实体的终端20是一个其中多个用户共享一台打印机或一个终端的装置时,签名信息和用于第二实体的第二加密可以包括所述签名信息和用于被公用的打印机或终端的加密系统。

即使没有来自用户终端20的请求,在所述合同信息的基础上,也可以在一个网络上或使用CD-ROM广泛地分发来自所述服务者终端10的第一被加密信息。

利用所述公共密钥加密方法不一定产生用于第二实体的签名信息S,可以在所提取信息的基础上产生由用户规定的信息(例如,代码号)。

在美国,为了使用用于40位或更多的加密,需要一个密钥管理办公室去管理加密密钥以避免所述密码未经授权的使用。因此,所述验证办公室也可以被用做为一个密钥管理办公室。当所述验证办公室对第二加密密钥提供一个超前管理时,所述验证办公室本身能够通过执行对非法图象的监视来进行验证处理1)和3)。第一实体的第一加密密钥可以通过同一个验证办公室进行管理,也可以通过另外一个密钥管理办公室进行管理。所述服务者和用户的密钥可以由密钥管理办公室产生和分发。

通过与处理1和2相关的代理可以执行相同的加密处理或使用不同加密方法或不同加密密钥的处理。

当所述服务者没有进行所述非法活动时,服务者或作者可以在图象数据中嵌入电子水印信息并将它分发给所述代理,所述代理可以嵌入不同的电子水印信息并将它分发给所述用户。

另外,代替单一的代理,可以分级提供多个代理来代替单一的代理。在这种情况下,负责分级结构的特定代理可以执行所述代理负责执行的处理,或各个代理可以执行所述协议以规定将要负责的一个代理。

如图 5 所示, 当只提供一个代理时, 可以省略涉及所述代理的用户信息 U1 的嵌入。

如上所述, 根据上述实施例的电子水印叠加方法和电子信息分发系统, 当相关的电子信息将被分发给三方中的至少一方时, 可以避免由于两方之间的共谋而引起的非法活动以及可以得到的这种共谋的一系列组合。

说明书附图

图 1

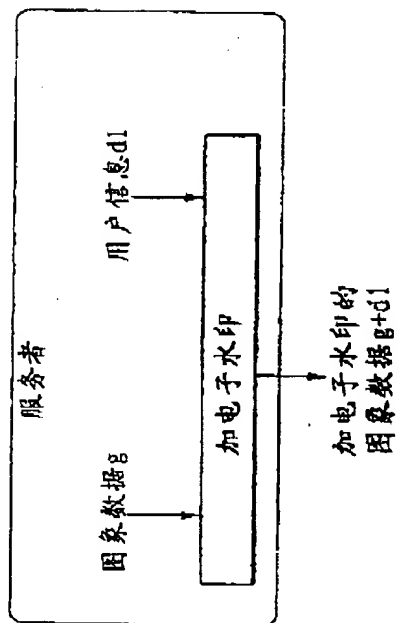


图 2

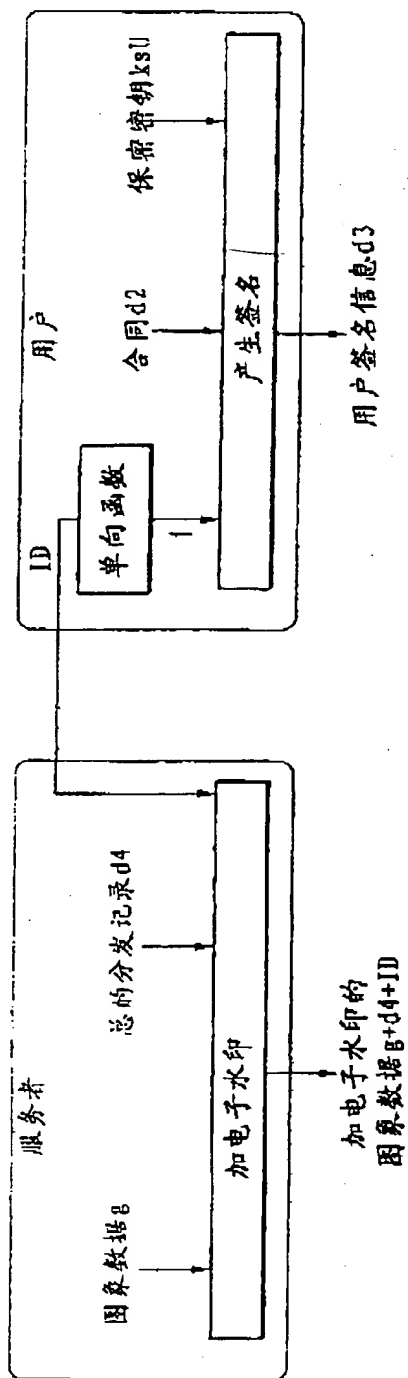


图 3

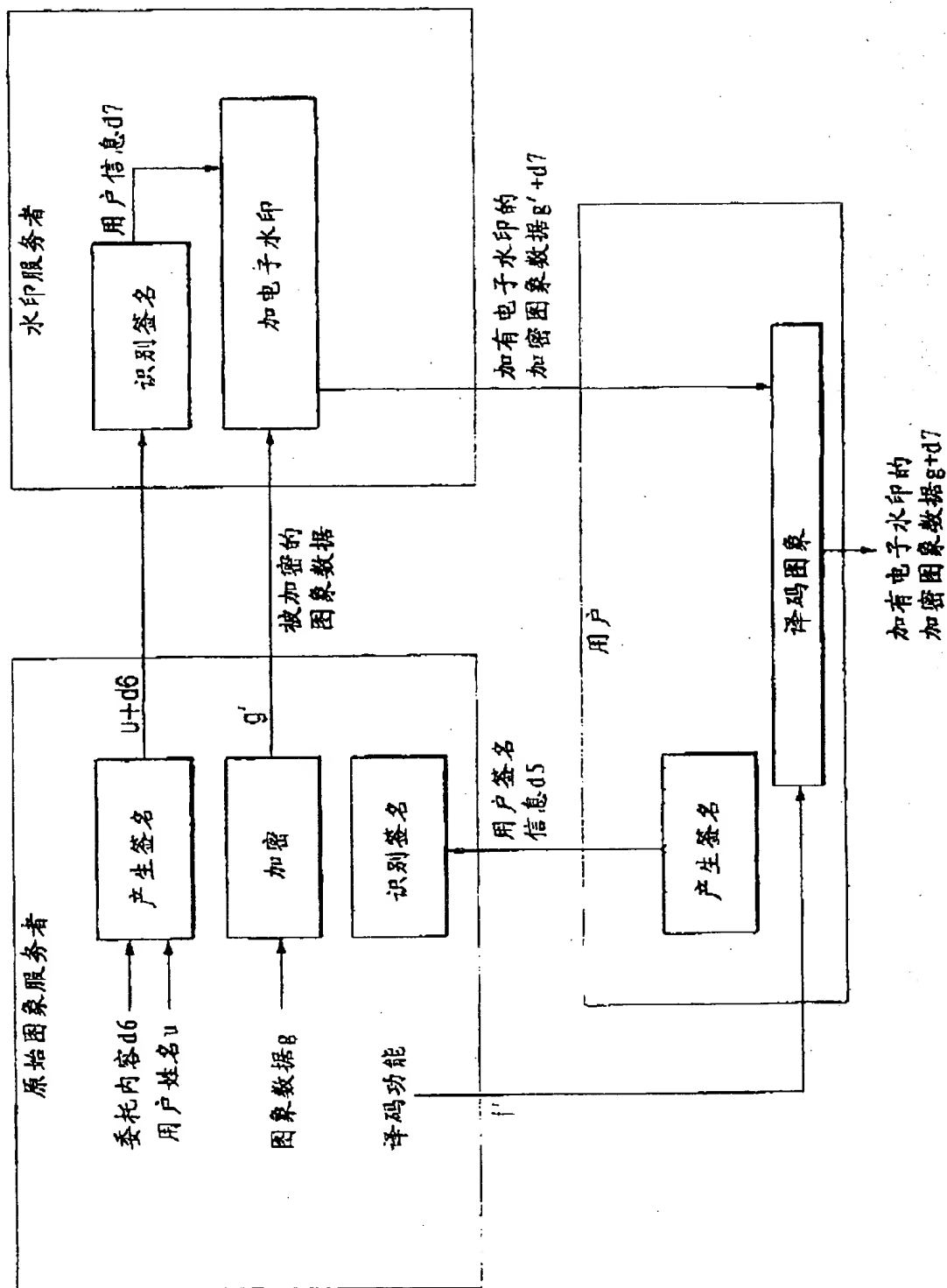


图 4

· 分级网络 (I) ·

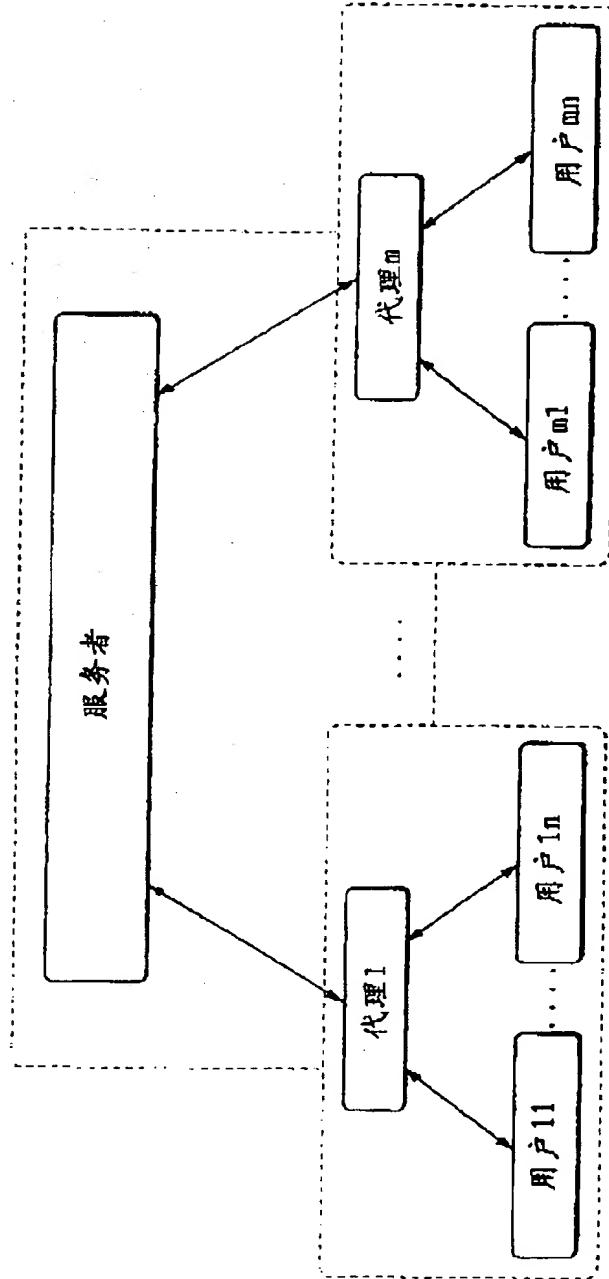
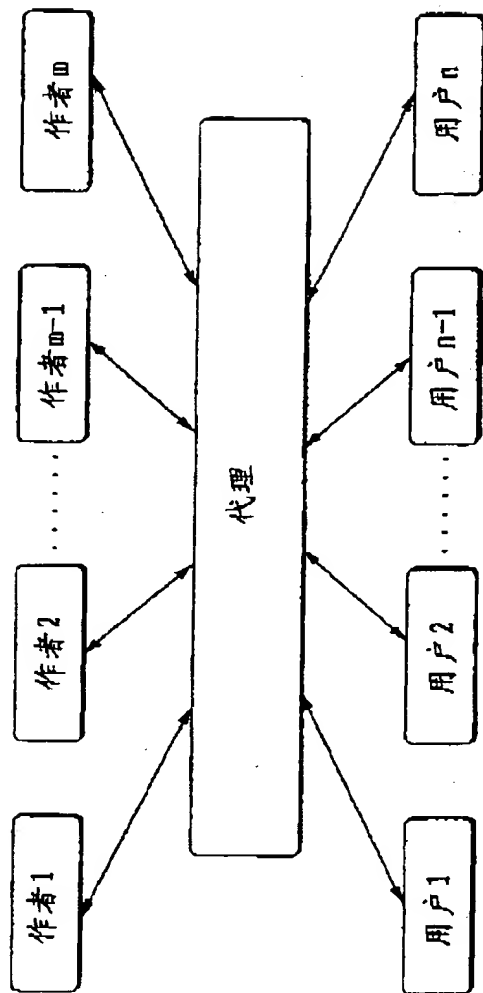


图 5

· 分级网络 (2)



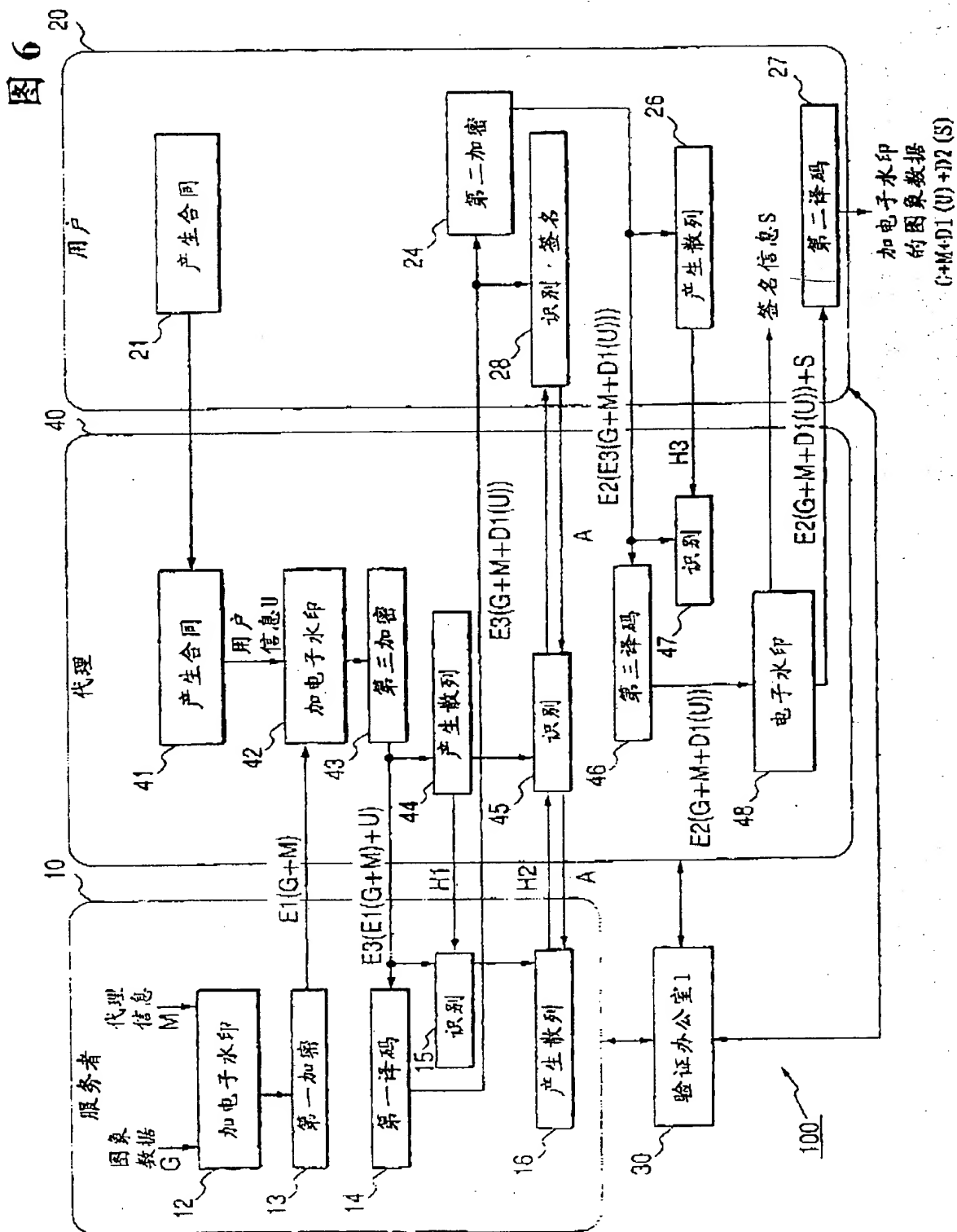
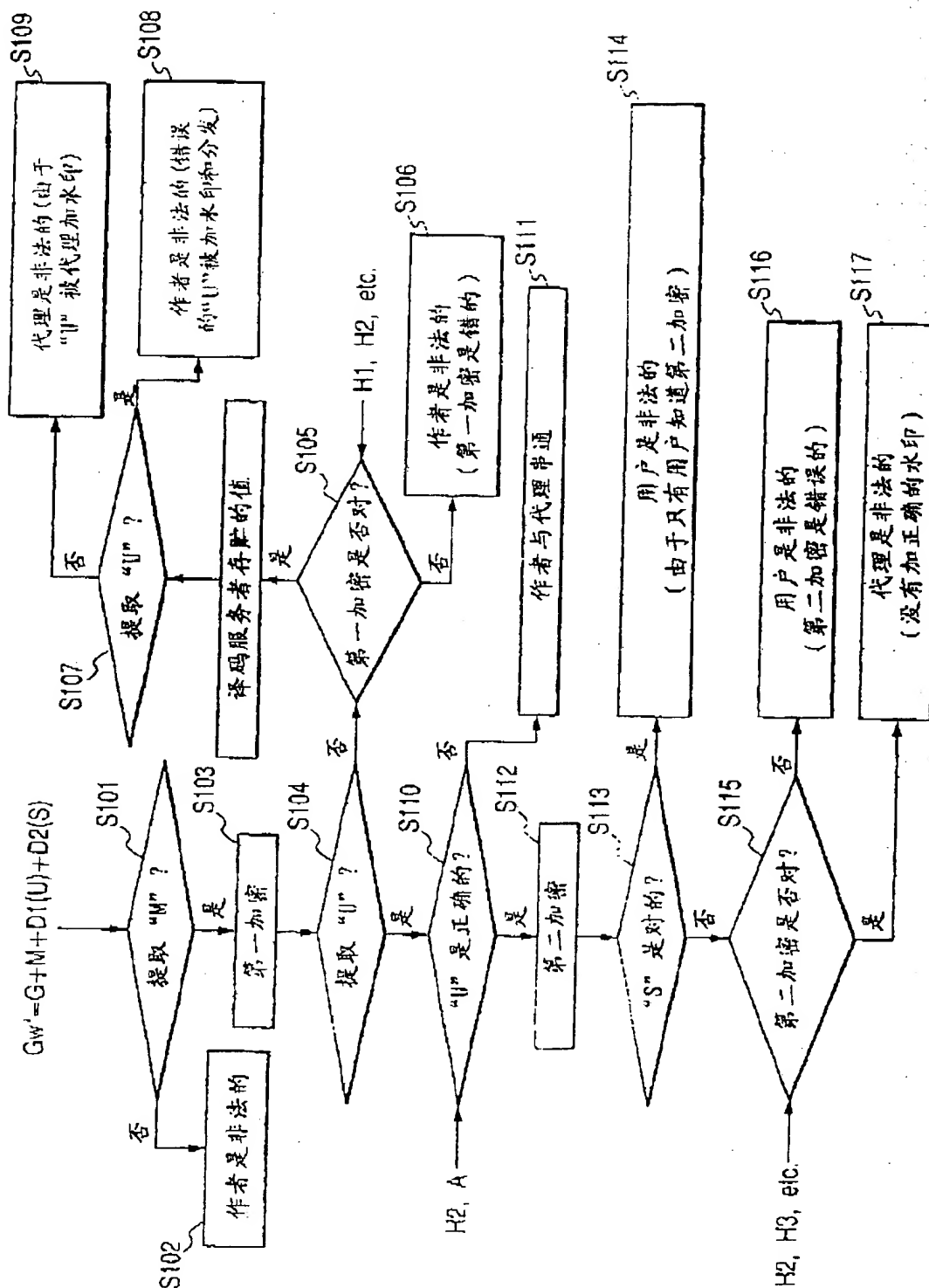


图 7



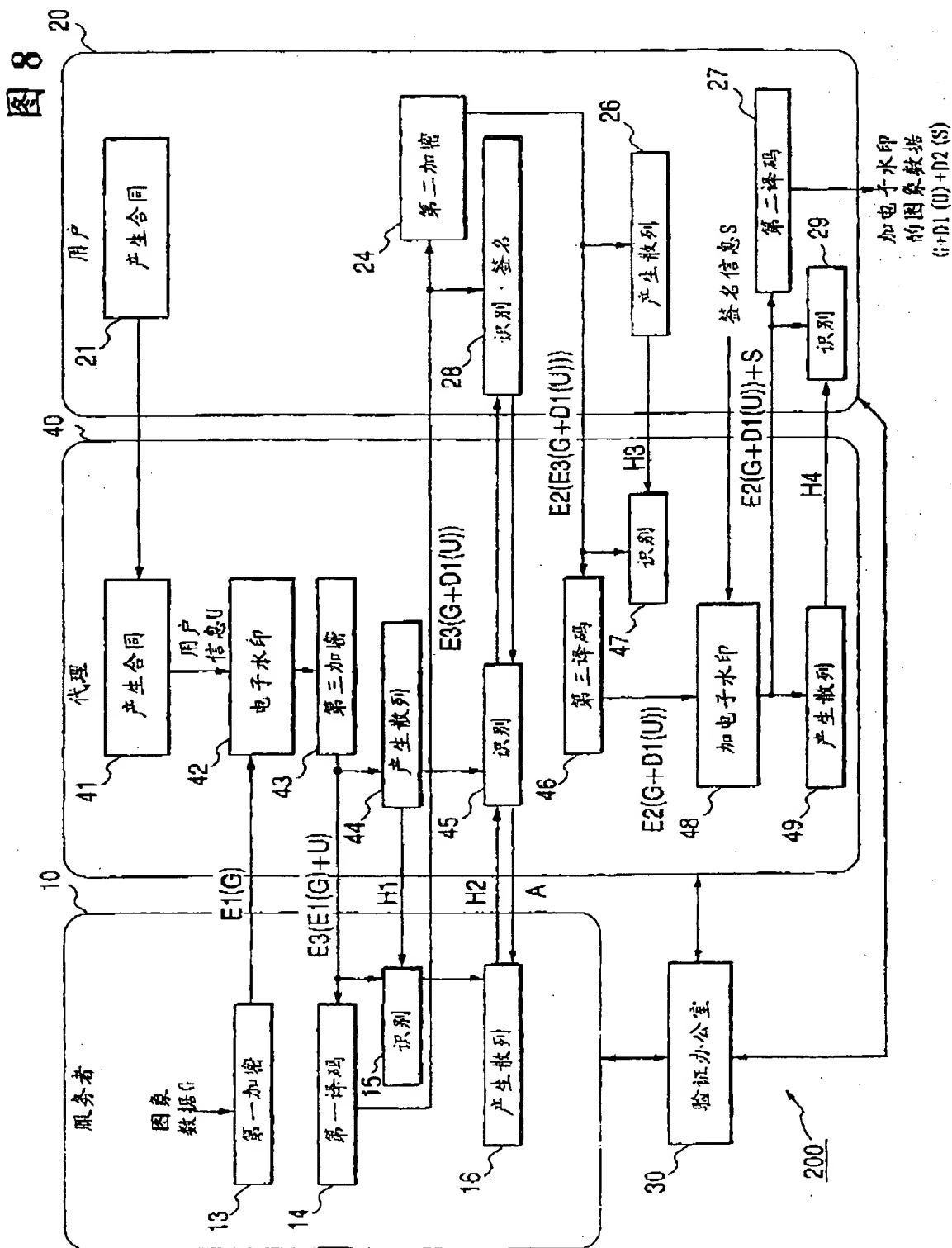


图 9

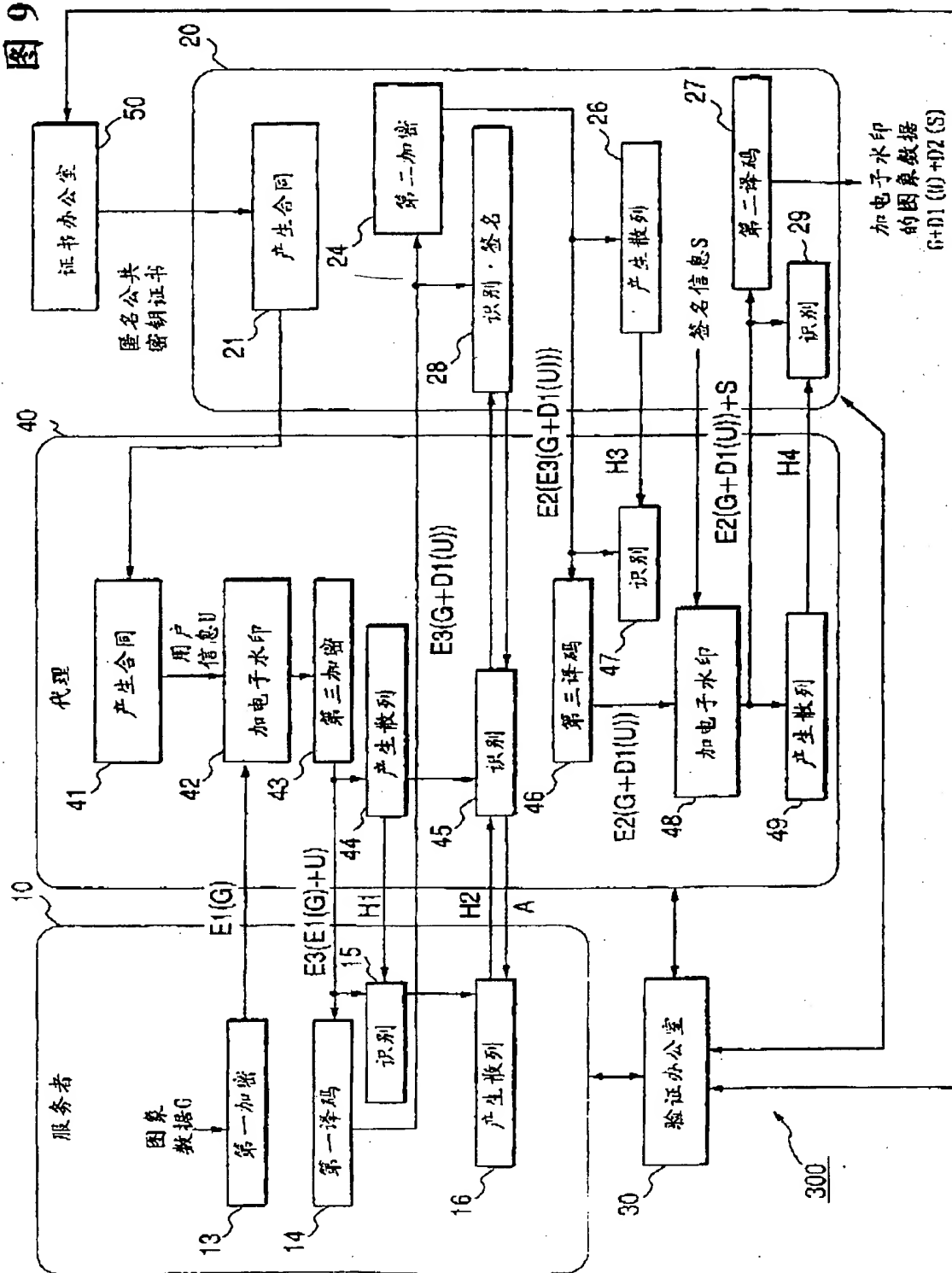


图 10

图 象 标 题 部 分	图 象 格 式 标 识 符
	文 件 大 小
	X 方 向 象 素 的 数 量 (宽 度)
	Y 方 向 象 素 的 数 量 (高 度)
	深 度 方 向 尺 寸
	压 缩 或 不 压 缩
	分 辨 率
	位 映 象 偏 移
	调 色 板 尺 寸
图 象 数 据 部 分	位 映 象

图 11

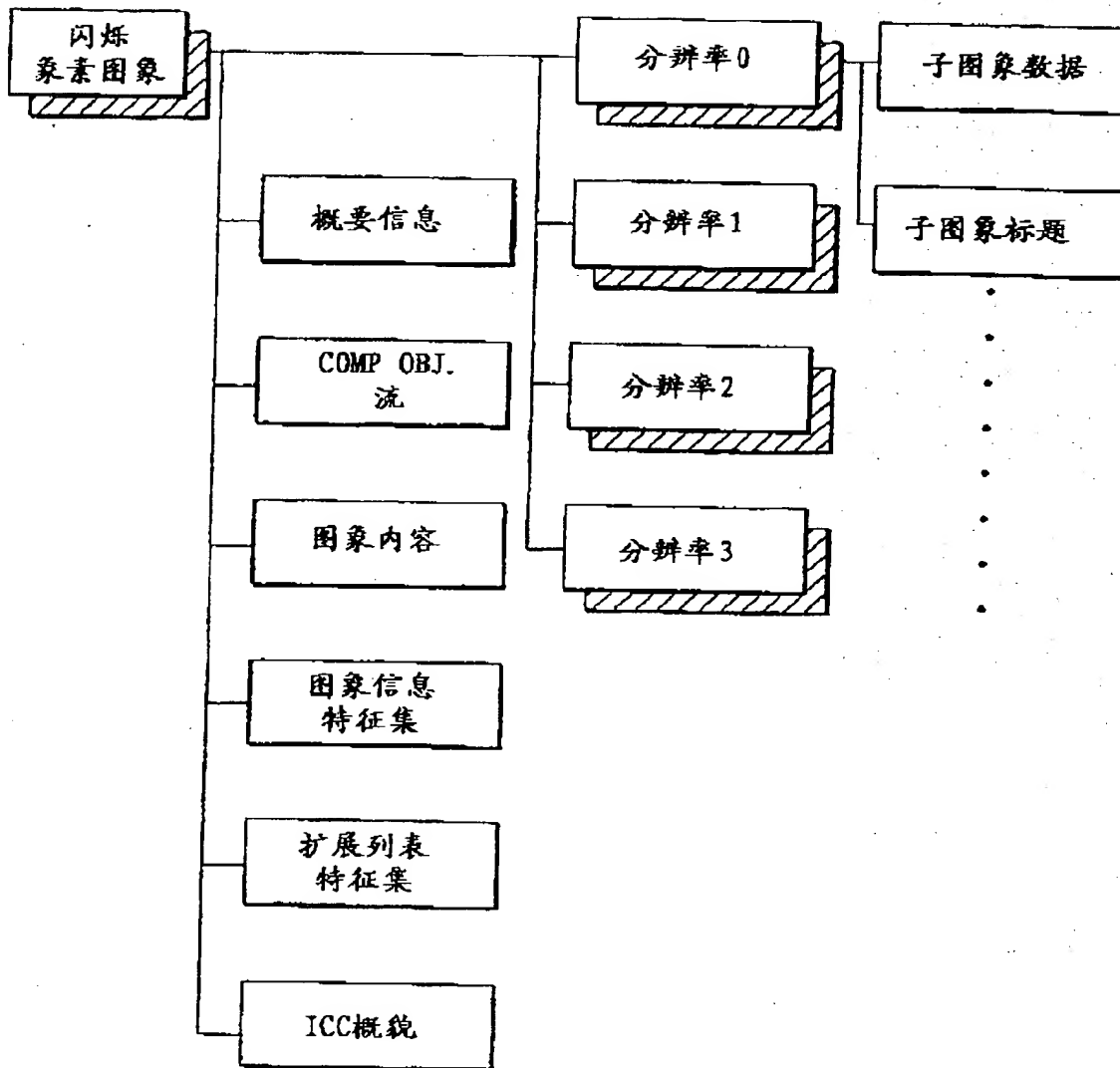


图 12

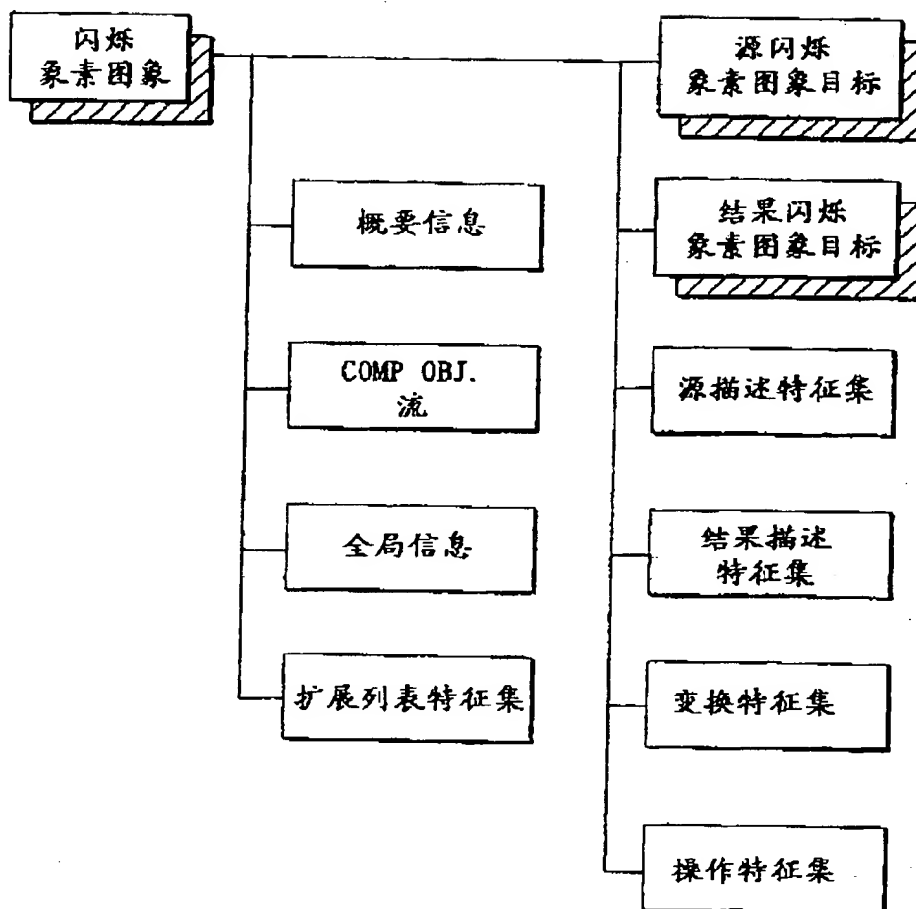


图 13

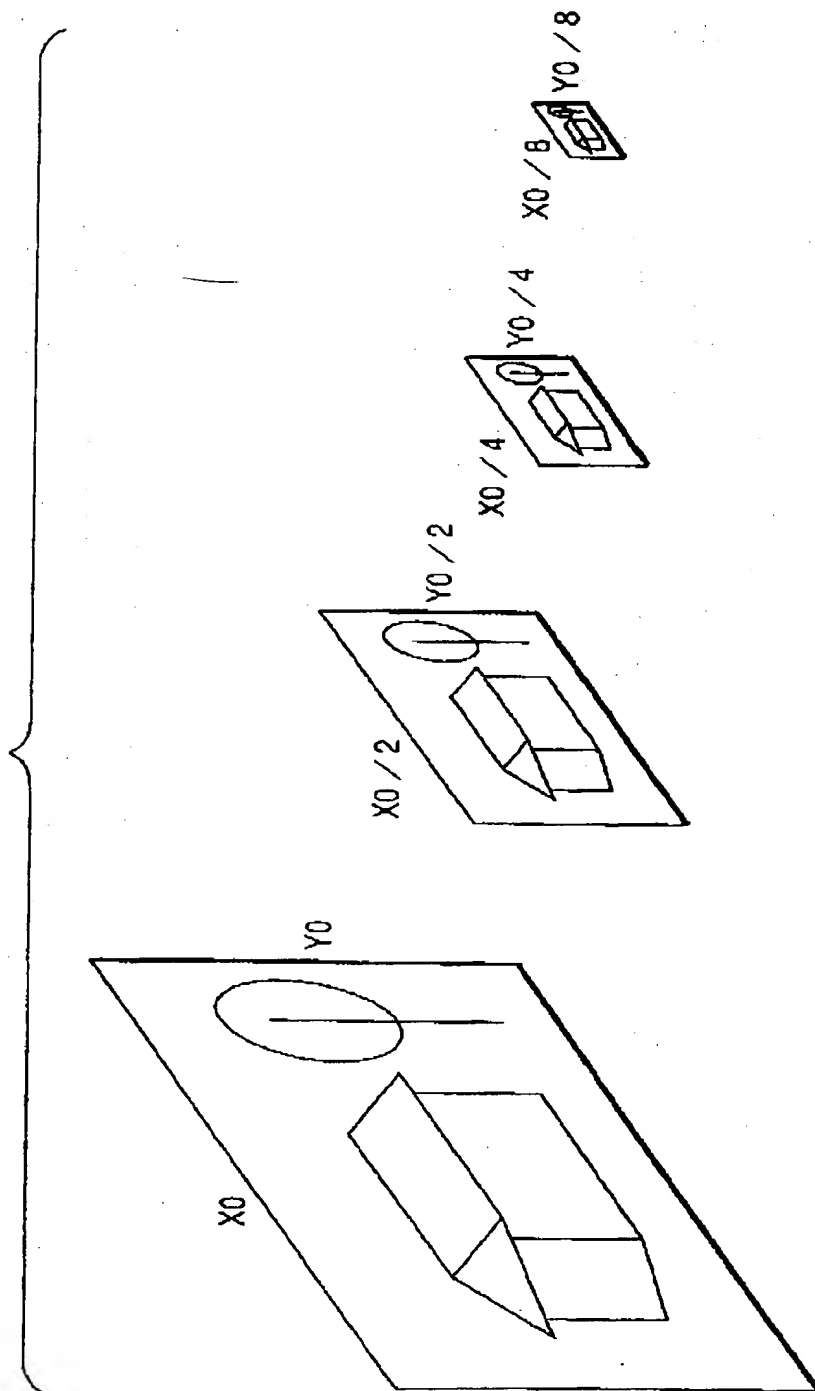
特征名	ID代码	类型
图象数据层数	0x01000000	VT_UI4
具有最大分辨率 的图象的宽度	0x01000002	VT_UI4
具有最大分辨率 的图象的高度	0x01000003	VT_UI4
最初显示高度	0x01000004	VT_R4
最初显示宽度	0x01000005	VT_R4

特征名	ID代码	类型
具有每个分辨率 的图象的宽度	0x02ii0000	VT_UI4
具有每个分辨率 的图象的高度	0x02ii0001	VT_UI4
具有每个分辨率 的图象的颜色	0x02ii0002	VT_BLOB
表达具有每个分辨率 的图象的格式	0x02ii0003	VT_UI4 VT_VECTOR

特征名	ID代码	类型
JPEG表	0x03ii0001	VT_BLOB
最大JPEG表的索引	0x03000002	VT_UI4

03-09-30

图 14



98-02-05

图 15

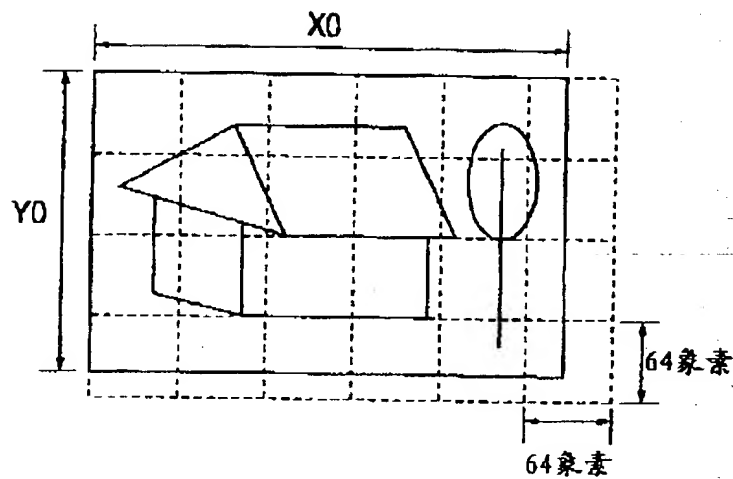


图 16

区域名	长度	字节
图象宽度	4	4-7
图象高度	4	8-11
铺砌的总数	4	12-15
铺砌宽度	4	16-19
铺砌高度	4	20-23

20 第二实体

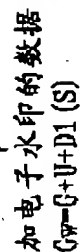
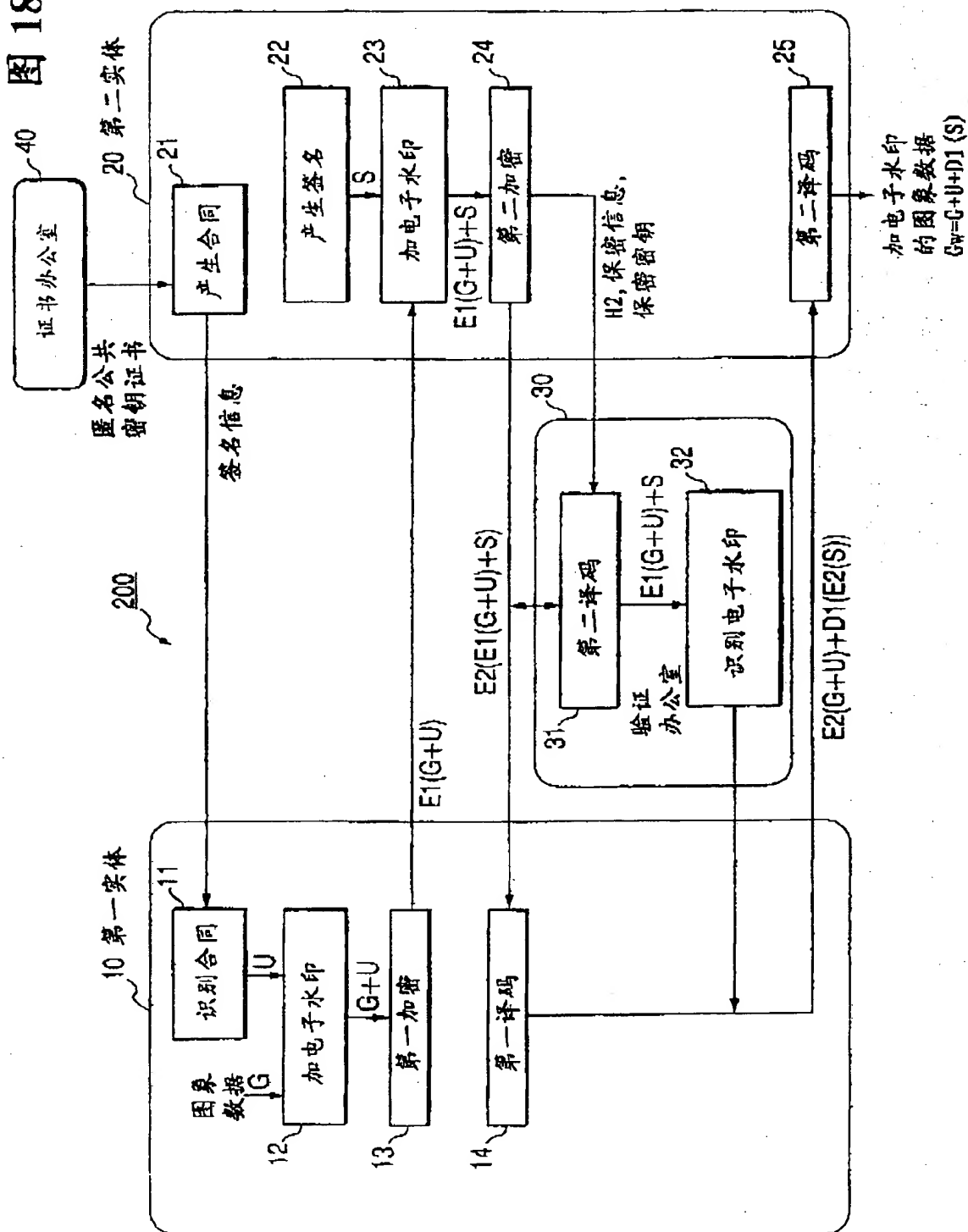
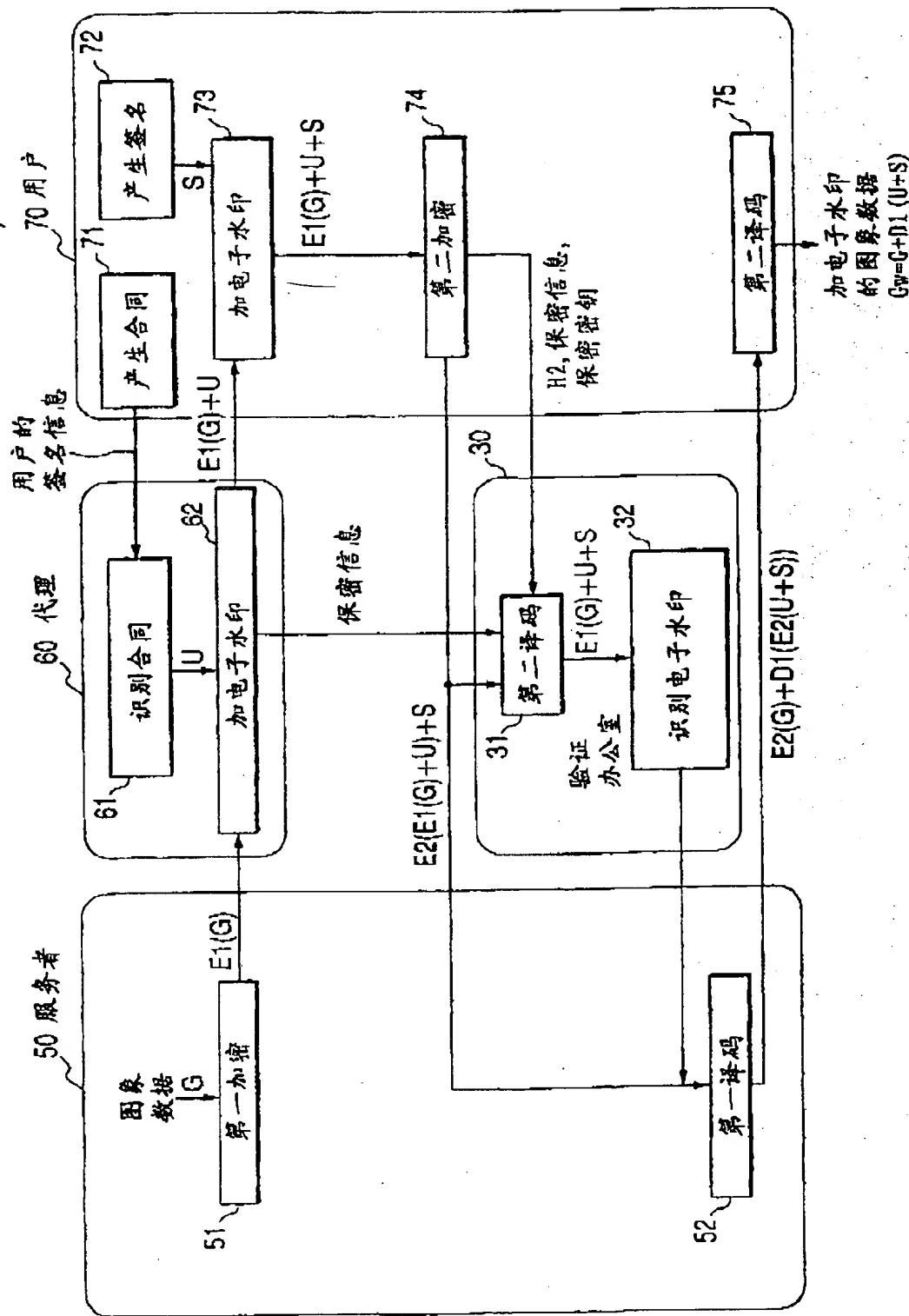
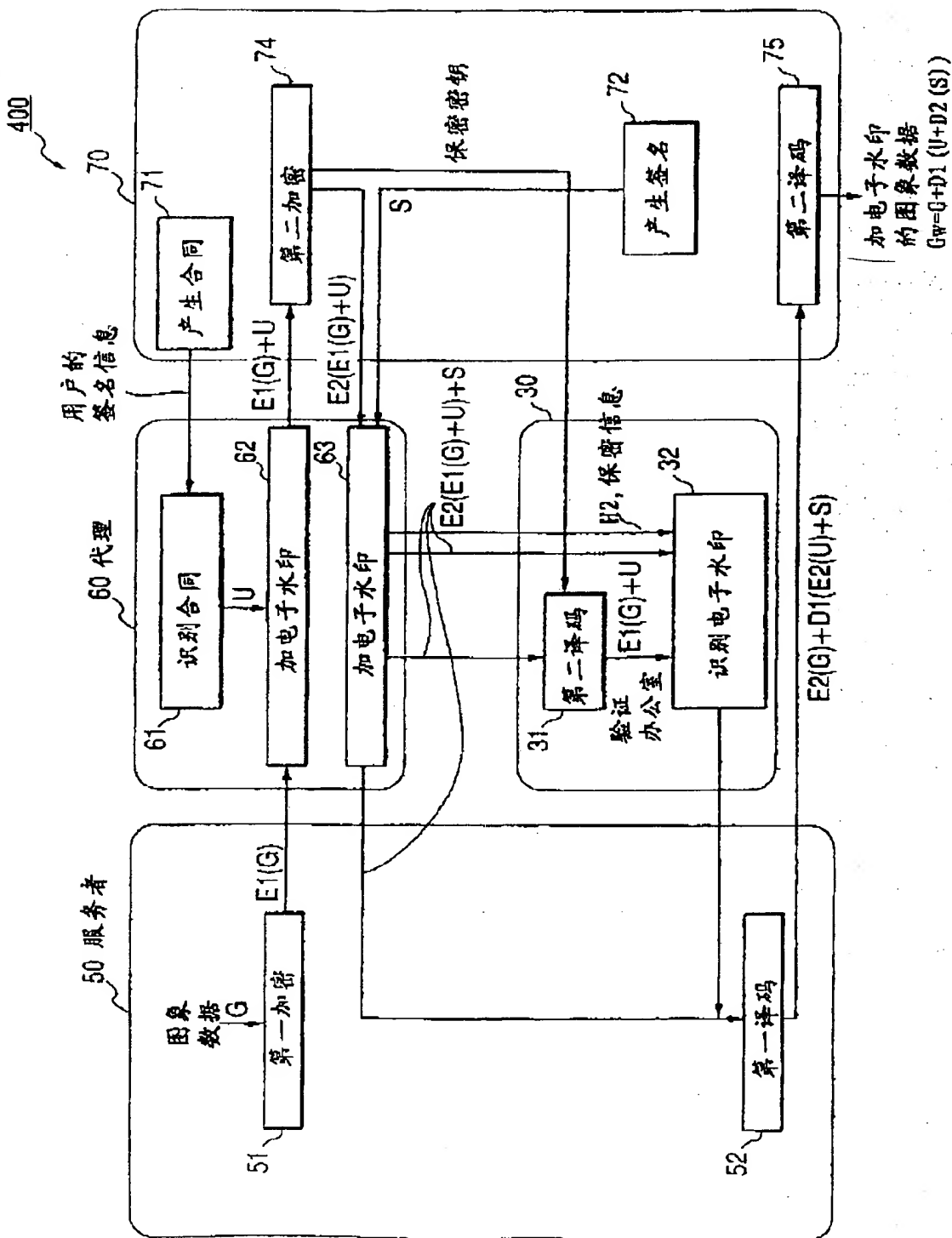


图 18



300 图 19



20
154

加电子水印
的图象数据
 $G_W = G + D1 (U + D2 (S))$

图 21

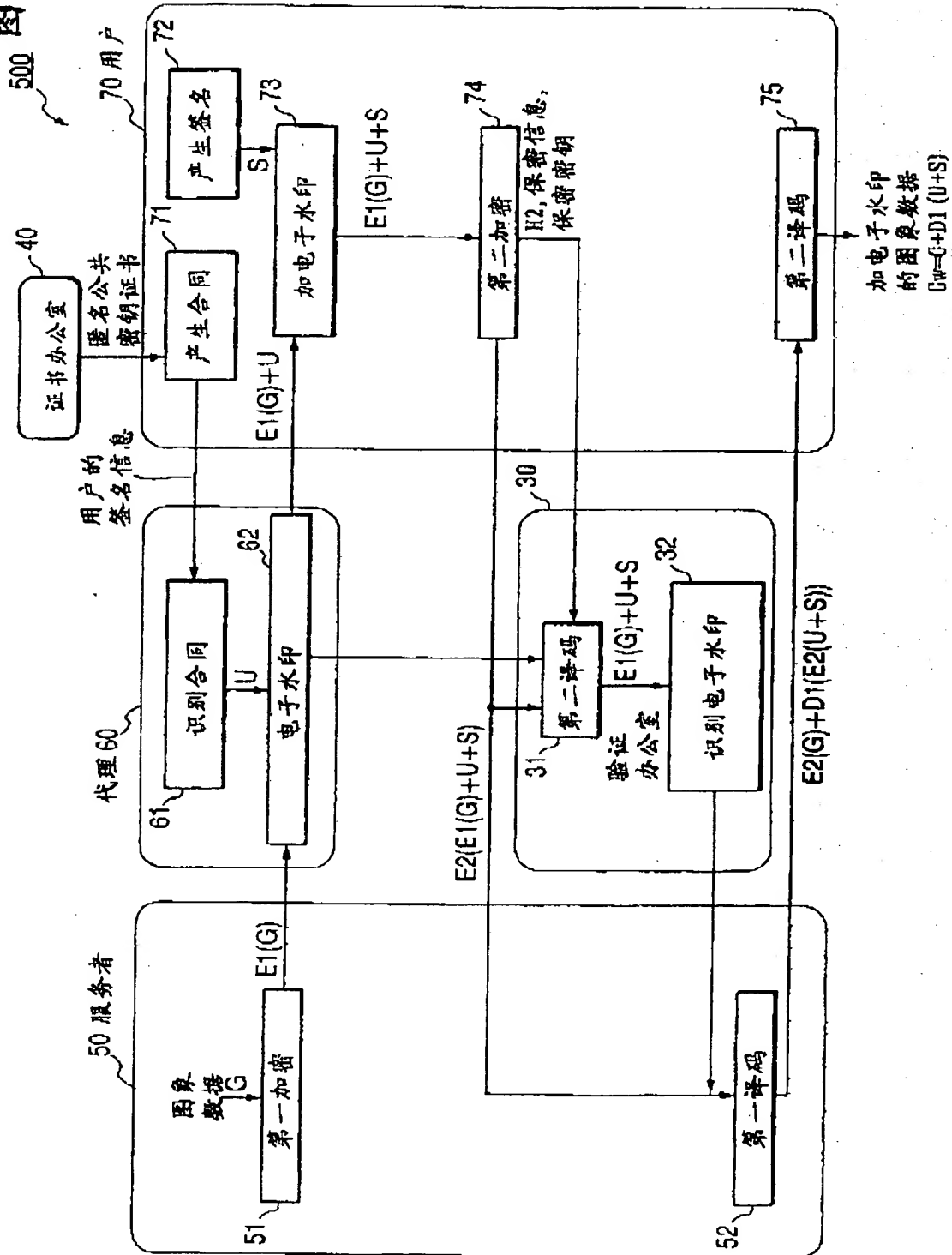


图 22

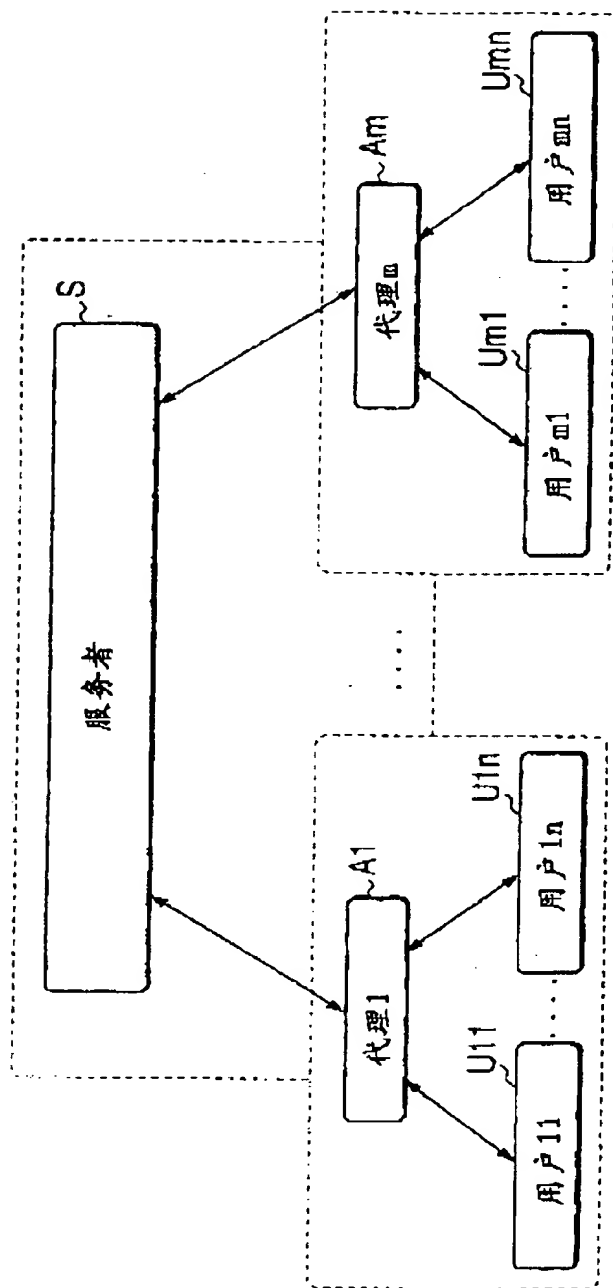


图 23

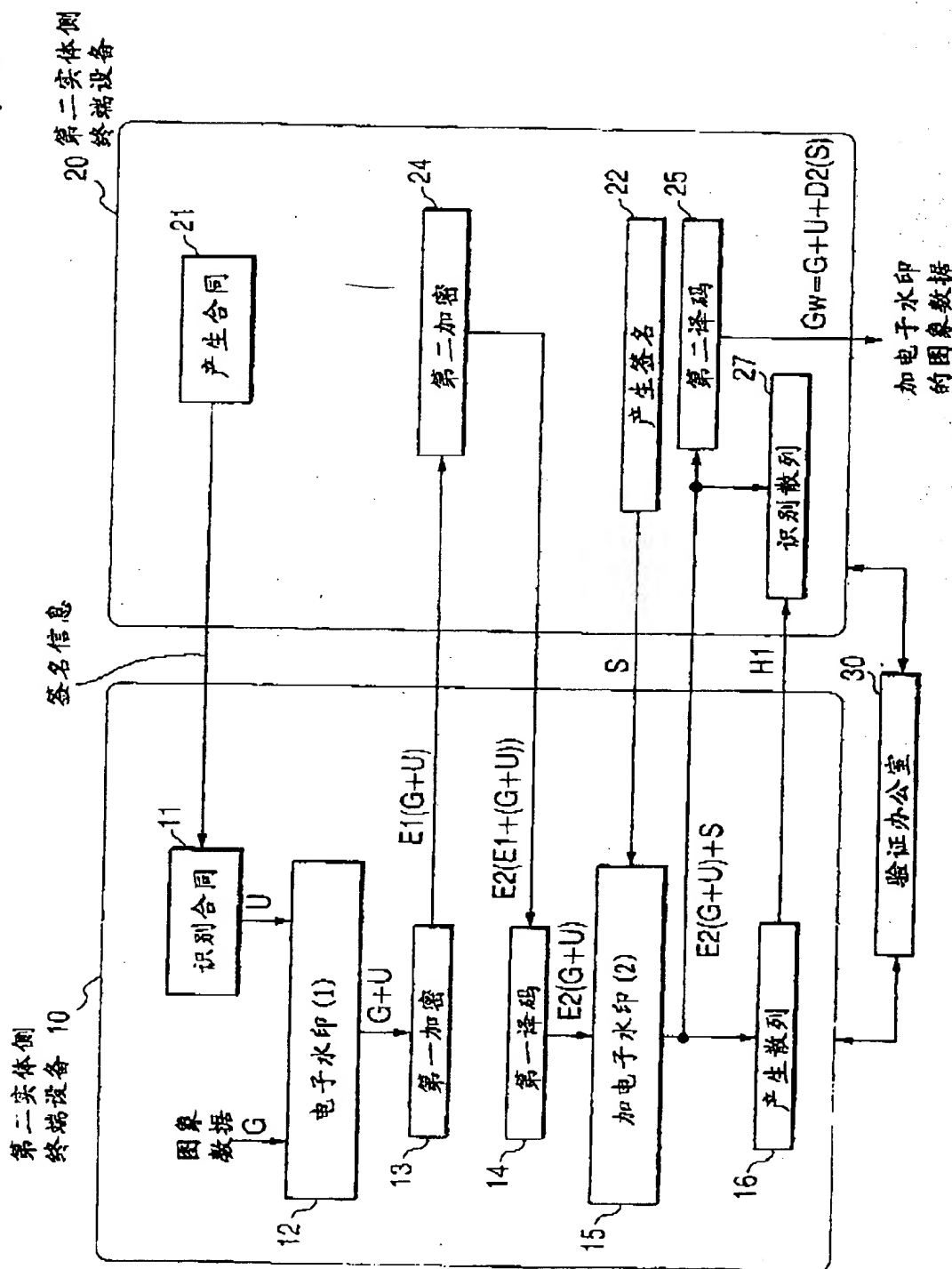


图 24

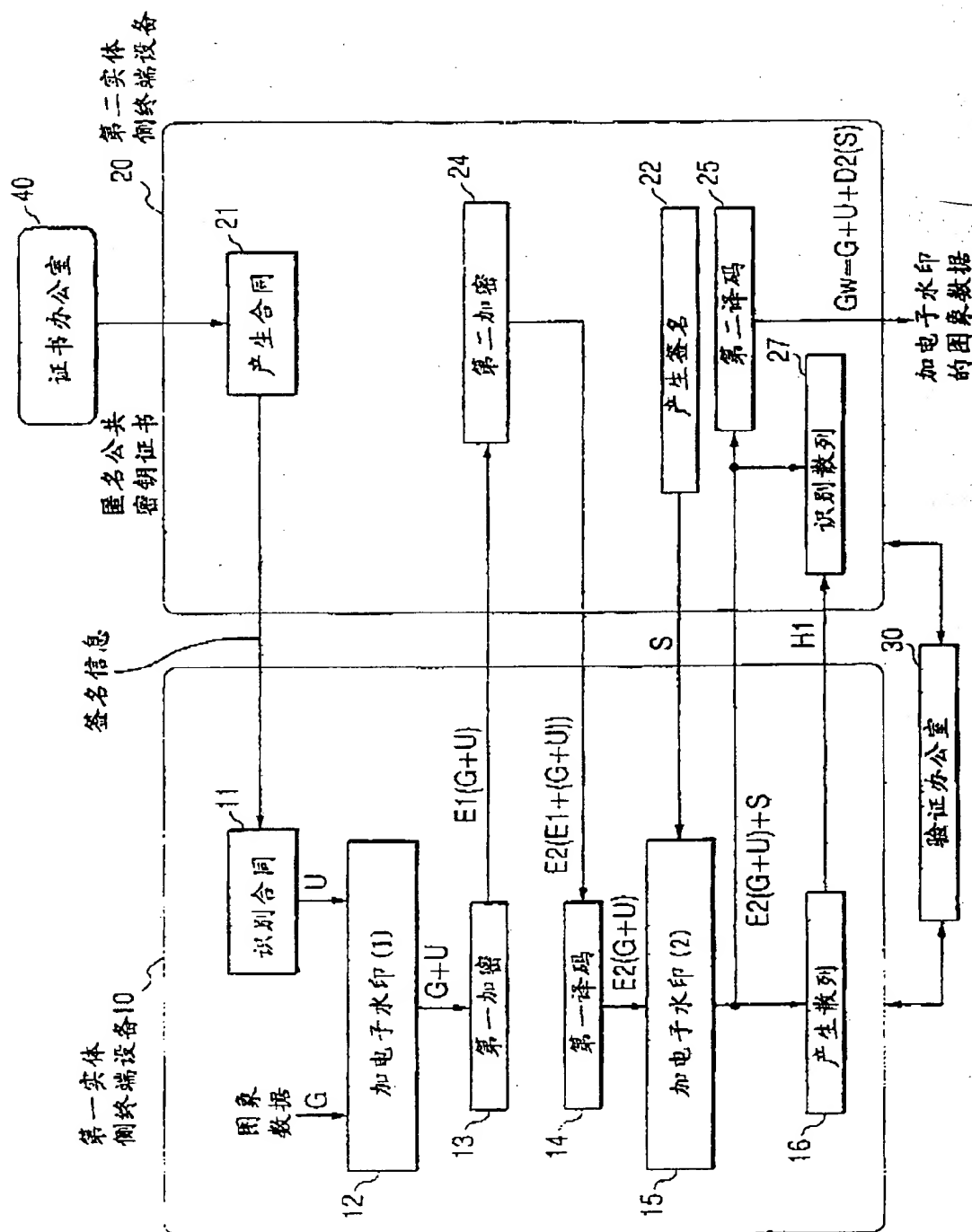


图 25

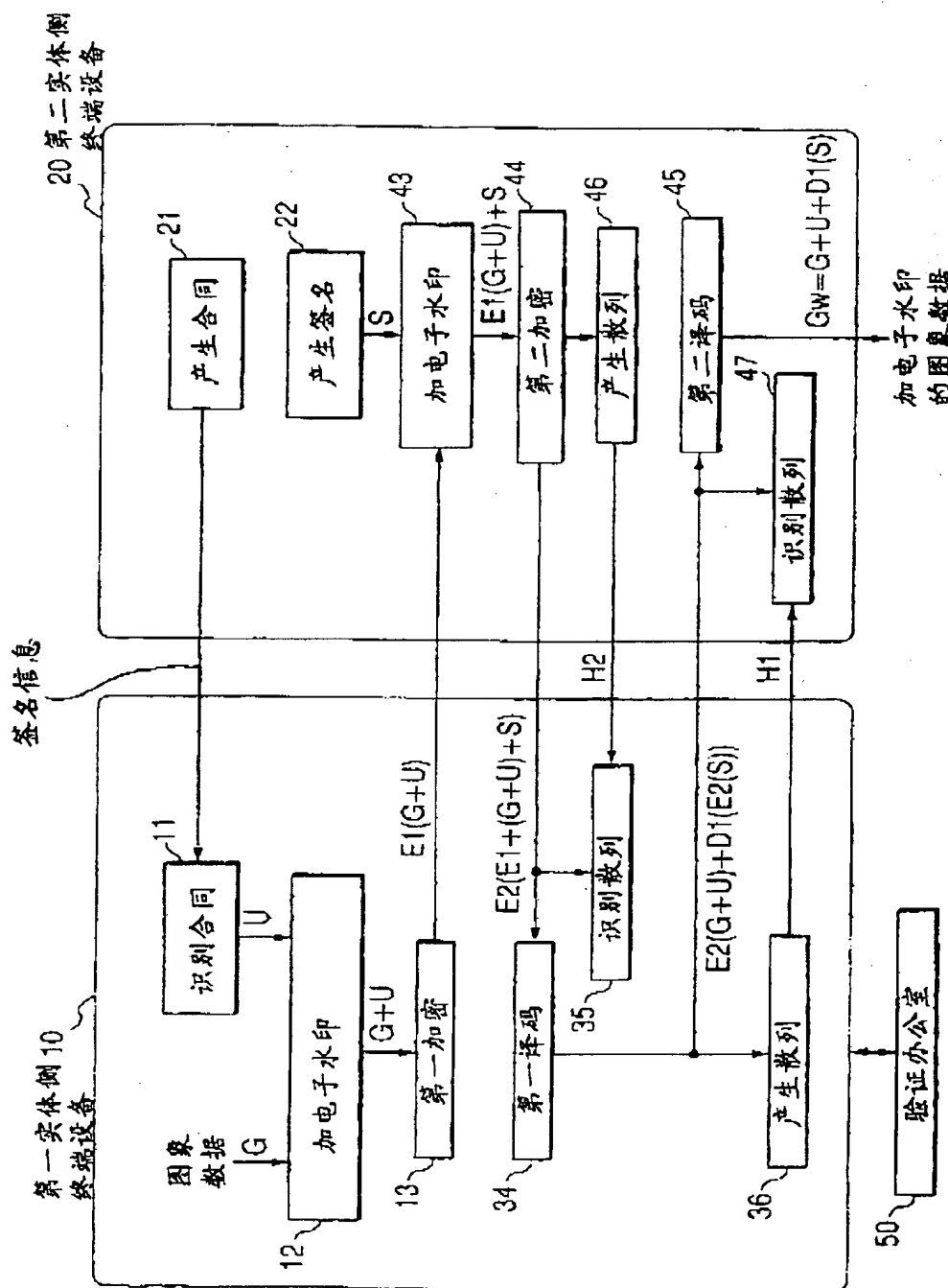


图 26

